WatchGuard® Firebox® SSL VPN Gateway Administration Guide

Firebox SSL VPN Gateway

Notice to Users

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Copyright, Trademark, and Patent Information

The Firebox SSL Firebox SSL VPN Gateway software is distributed with source code covered under the GNU General Public License (GPL). To obtain source code covered under the GPL, please contact WatchGuard Technical Support at:

877.232.3531 in the United States and Canada
+1.206.613.0456 in all other countries

This source code is free to download. There is a $35 charge to ship the CD.

See Appendix E, "Legal and Copyright Information" on page 173 of this guide for the complete text of the GPL.

VPN Gateway Software: 5.5
Document Version: 352-2784-001

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

SUPPORT:
www.watchguard.com/support
support@watchguard.com
U.S. and Canada +877.232.3531
All Other Countries +1.206.613.0456

SALES:
U.S. and Canada +1.800.734.9905
All Other Countries +1.206.521.8340

ABOUT WATCHGUARD

WatchGuard is a leading provider of network security solutions for small- to mid-sized enterprises worldwide, delivering integrated products and services that are robust as well as easy to buy, deploy and manage. The company's Firebox X family of expandable integrated security appliances is designed to be fully upgradeable as an organization grows and to deliver the industry's best combination of security, performance, intuitive interface and value. WatchGuard Intelligent Layered Security architecture protects against emerging threats effectively and efficiently and provides the flexibility to integrate additional security functionality and services offered through WatchGuard. Every WatchGuard product comes with an initial LiveSecurity Service subscription to help customers stay on top of the security landscape with vulnerability alerts, software updates, expert security instruction and superior customer care. For more information, please call (206) 521-8340 or visit www.watchguard.com.

Contents

CHAPTER 1

Getting Started with Firebox SSL VPN Gateway

This chapter describes who should read the *Firebox SSL VPN Gateway Administration Guide*, how it is organized, and its document conventions.

Audience

This user guide is intended for system administrators responsible for installing and configuring the Firebox SSL VPN Gateway. This document assumes that the Firebox SSL VPN Gateway is connected to an existing network and that the administrator has experience configuring that network.

Operating System Requirements

The Firebox SSL VPN Gateway Administration Tool and Secure Access Client software can run on the following operating systems:

- Windows 2000 Professional
- Windows 2000 Server
- Windows XP Home Edition
- Windows XP Professional
- Windows Server 2003
- Windows Vista 32-bit
- Linux 2.4 platforms (all distributions)

Document Conventions

Firebox SSL VPN Gateway documentation uses the following typographic conventions for menus, commands, keyboard keys, and items in the program interface:

Convention	Meaning
Boldface	Commands, names of interface items such as text boxes, option buttons, and user input.
Italics	Placeholders for information or parameters that you provide. For example, *filename* in a procedure means you type the actual name of a file. Italics also are used for new terms and the titles of books.
%SystemRoot%	The Windows system directory, which can be WTSRV, WINNT, WINDOWS, or other name you specify when you install Windows.
Monospace	Text displayed in a text file.
{ braces }	A series of items, one of which is required in command statements. For example, **{ yes | no }** means you must type **yes** or **no**. Do not type the braces themselves.
[brackets]	Optional items in command statements. For example, [**/ping**] means that you can type **/ping** with the command. Do not type the brackets themselves.
| (vertical bar)	A separator between items in braces or brackets in command statements. For example, **{ /hold | /release | /delete }** means you type **/hold** or **/release** or **/delete**.
… (ellipsis)	You can repeat the previous item or items in command statements. For example, **/route:***devicename*[,…] means you can type additional *devicenames* separated by commas.

LiveSecurity Service Solutions

The number of new security problems and the volume of information about network security continues to increase. We know that a firewall is only the first component in a full security solution. The WatchGuard® Rapid Response Team is a dedicated group of network security personnel who can help you to control the problem of too much security information. They monitor the Internet security web sites to identify new security problems.

Threat responses, alerts, and expert advice

After a new threat is identified, the WatchGuard Rapid Response Team sends you an e-mail to tell you about the problem. Each message gives full information about the type of security problem and the procedure you must use to make sure that your network is safe from attack.

Easy software updates

LiveSecurity® Service saves you time because you receive an e-mail when we release new version of your software. These continued updates make sure that you do not have to use your time to find new software.

Access to technical support and training

You can find information about your WatchGuard products quickly with our many online resources. You can also speak directly to one of the WatchGuard technical support personnel. Use our online training to

learn more about your WatchGuard Firebox® and network security, or find a WatchGuard Certified Training Center in your area.

LiveSecurity Service Broadcasts

The WatchGuard® Rapid Response Team regularly sends messages and software information directly to your computer desktop by e-mail. We divide the messages into categories to help you to identify and make use of incoming information immediately.

Information Alert

Information Alerts give you a fast view of the newest information and threats to Internet security. The WatchGuard Rapid Response Team frequently recommends that you make a security policy change to protect against the new threat. When necessary, the Information Alert includes instructions on the procedure.

Threat Response

If a new security threat makes it necessary, the WatchGuard Rapid Response Team transmits a software update for your Firebox®. The Threat Response includes information about the security threat and instructions on how to download a software update and install it on your Firebox and management station.

Software Update

When necessary, WatchGuard updates the WatchGuard System Manager software. Product upgrades can include new features and patches. When we release a software update, you get an e-mail with instructions on how to download and install your upgrade.

Editorial

Each week, top network security personnel come together with the WatchGuard Rapid Response Team to write about network security. This continuous supply of information can help your network be safe and secure.

Foundations

The WatchGuard Rapid Response Team also writes information specially for security administrators, employees, and other personnel that are new to this technology.

Loopback

At the end of each month LiveSecurity® Service sends you an e-mail with a summary of the information sent that month.

Support Flash

These short training messages can help you to operate WatchGuard products. They are an added resource to the other online resources:

- Online Help
- FAQs
- Known Issues pages on the Technical Support web site

Virus Alert

WatchGuard has come together with antivirus vendor McAfee to give you the most current information about computer viruses. Each week, we send you a message with a summary of the virus traffic on the Internet. When a hacker releases a dangerous virus on the Internet, we send a special virus alert to help you protect your network.

New from WatchGuard

When WatchGuard releases a new product, we first tell you — our customers. You can learn about new features and services, product upgrades, hardware releases, and promotions.

Activating LiveSecurity Service

You can activate LiveSecurity® Service through the activation section of the LiveSecurity web pages.

Note

To activate LiveSecurity Service, you must enable JavaScript on your browser.

To activate LiveSecurity Service through the Internet:

1 Make sure that you have your Firebox® serial number. This is necessary during the LiveSecurity activation procedure.
   - You can find the Firebox serial number on a label on the rear side of the Firebox below the Universal Product Code (UPC), or on a label on the bottom of the Firebox.
   - The license key numbers for LiveSecurity and LiveSecurity Tunnel Renewals are on the WatchGuard LiveSecurity License Key certificate. Make sure that you enter the license key in all capital letters and include hyphens.

2 Use your web browser to go to:
www.watchguard.com/account/register.asp
The Account page appears.

3 Complete the LiveSecurity Activation page. Use the TAB key or the mouse to move through the fields on the page.
You must complete all the fields to activate correctly. This information helps WatchGuard to send you the information and software updates that are applicable to your products.

4 Make sure that your e-mail address is correct. Your LiveSecurity e-mails about product updates and threat responses come to this address. After you complete the procedure, you get an e-mail message that tells you that you activated LiveSecurity Service succesfully.

5 Click **Register**.

LiveSecurity Service Self Help Tools

Online Self Help Tools enable you to get the best performance from your WatchGuard® products.

Note

You must activate LiveSecurity® Service before you can access online resources.

Instant Answers

Instant Answers is a guided Help tool designed to give solutions to product questions very quickly. Instant Answers asks you questions and then gives you to the best solution based on the answers you give.

Basic FAQs

The Basic FAQs (frequently asked questions) give you general information about the Firebox® and the WatchGuard System Manager software. They are written for the customer who is new to network security and to WatchGuard products.

Advanced FAQs

The Advanced FAQs (frequently asked questions) give you important information about configuration options and operation of systems or products. They add to the information you can find in this User Guide and in the Online Help system.

Fireware® "How To"'s

The Fireware How To documentation helps you to quickly find procedures for configuration tasks specific to Fireware appliance software.

Known Issues

This Known Issues tool monitors WatchGuard product problems and software updates.

WatchGuard Users Forum

The WatchGuard Technical Support team operates a web site where customers can help each other with WatchGuard products. Technical Support monitors this forum to make sure you get accurate information.

Online Training

Browse to the online training section to learn more about network security and WatchGuard products. You can read training materials and get a certification in WatchGuard products. The training includes links to a wide range of documents and web sites about network security. The training is divided into parts, which lets you use only the materials you feel necessary. To learn more about online training, browse to:
www.watchguard.com/training/courses_online.asp

Learn About

Learn About is a list of all resources available for a specified product or feature. It is a site map for the feature.

Product Documentation

The WatchGuard web site has a copy of each product user guide, including user guides for software versions that are no longer supported. The user guides are in .pdf format.

General Firebox X Edge and Firebox SOHO Resources

This section of the web site shows basic information and links for Firebox X Edge and Firebox SOHO customers. It can help you to install and use the Firebox X Edge and SOHO hardware.

To get access to the LiveSecurity Service Self Help Tools:

1 Start your web browser. In the address bar, type:
http://www.watchguard.com/support

2 Click **Self Help Tools**.
You must log in.

3 Click your selection.

WatchGuard Users Forum

The WatchGuard® Users Forum is an online group. It lets users of WatchGuard products interchange product information about:

- Configuration
- Connecting WatchGuard products and those of other companies
- Network policies

This forum has different categories that you can use to look for information. The Technical Support team controls the forum during regular work hours. You do not get special help from Technical Support when you use the forum. To contact Technical Support directly from the web, log in to your LiveSecurity account. Click on the **Incidents** link to send a Technical Support incident.

Using the WatchGuard Users Forum

To use the WatchGuard Users Forum you must first create an account. Browse to http://www.watchguard.com/forum for instructions.

Online Help

Online Help for the Firebox SSL VPN Gateway is included in the application software. It is available in the pane on the left side of your application window.

Product Documentation

We copy all user guides to the web site at http://www.watchguard.com/help/documentation.

Technical Support

Your LiveSecurity® Service subscription includes technical support for the WatchGuard® System Manager software and Firebox® hardware. To learn more about WatchGuard Technical Support, browse to the WatchGuard web site at:

http://www.watchguard.com/support

Note

You must activate LiveSecurity Service before you can get technical support.

LiveSecurity Service technical support

All new Firebox products include the WatchGuard LiveSecurity Technical Support Service. You can speak with a member of the WatchGuard Technical Support team when you have a problem with the installation, management, or configuration of your Firebox.

Hours

WatchGuard LiveSecurity Technical Support operates from 6:00 AM to 6:00 PM in your local time zone, Monday through Friday.

Telephone number

877.232.3531 (select option #2) in United States and Canada
+1.206.613.0456 in all other countries

Web site

http://www.watchguard.com/support

Service time

We try for a maximum response time of four hours.

Single Incident Priority Response Upgrade (SIPRU) and Single Incident After Hours Upgrade (SIAU) are also available. For more data about these upgrades, refer to the WatchGuard web site at:

http://www.watchguard.com/support

LiveSecurity Gold

WatchGuard Gold LiveSecurity Technical Support adds to your standard LiveSecurity Service. We recommend that you get this upgrade if you use the Internet or VPN tunnels for most of your work.

With WatchGuard Gold LiveSecurity Technical Support you get:

- Technical support 24 hours a day, seven days a week, including holidays.
- The Technical Support Team operates the support center from 7 PM Sunday to 7 PM Friday (Pacific Time). For weekend support for critical problems, use the on-call paging system.
- We try for a maximum response time of one hour.
- To create a support incident, call WatchGuard LiveSecurity Technical Support. A Customer Care representative records the problem and gives you an incident number. A Priority Support technician calls you as quickly as possible. If you have a critical problem when the support center is not open, use the LiveSecurity Technical Support phone number to page a technician. You can also send an incident on the web site at: http://www.watchguard.com/support/incidents/newincident.asp.

Firebox Installation Service

WatchGuard Remote Firebox Installation Service helps you to install and configure your Firebox. You can schedule two hours with a WatchGuard Technical Support team member. The technician helps you to:

- Do an analysis of your network and security policy
- Install the WatchGuard System Manager software and Firebox hardware
- Align your configuration with your company security policy

This service does not include VPN installation.

VPN Installation Service

WatchGuard Remote VPN Installation Service helps you through a full VPN installation. You can schedule a two-hour time with one of the WatchGuard Technical Support team. During this time, the technician helps:

- Do an analysis of your VPN policy
- Configure your VPN tunnels
- Do a test of your VPN configuration

You can use this service after you correctly install and configure your Firebox devices.

Training and Certification

WatchGuard® product training is available online to help you learn more about network security and WatchGuard products. You can find training materials on the Technical Support web site and prepare for

a certification exam. The training materials include links to books and web sites with more information about network security.

WatchGuard product training is also available at a location near you through a large group of WatchGuard Certified Training Partners (WCTPs). Training partners give training using certified training materials and with WatchGuard hardware. You can install and configure the products with an advanced instructor and system administrator to help you learn. To find a training partner, go to http://www.watchguard.com/training/partners_locate.asp

CHAPTER 2

Introduction to Firebox SSL VPN Gateway

WatchGuard Firebox SSL VPN Gateway is a universal Secure Socket Layer (SSL) virtual private network (VPN) appliance that provides a secure single point-of-access to any information resource — both data and voice. Combining the best features of Internet Protocol Security (IPSec) and SSL VPN, without the costly and cumbersome implementation and management, Firebox SSL VPN Gateway works through any firewall and supports all applications and protocols. It is fast, simple, and cost-effective to deploy and maintain with a Web-deployed and automatically updating client. Users receive a consistent desk-like user experience with "always-on" connectivity, an integrated worm-blocking client, and integrated end-point scanning. With the Firebox SSL VPN Gateway, organizations can quickly and easily deploy one product for all of their secure remote access needs.

The Firebox SSL VPN Gateway gives the remote user seamless, secure access to authorized applications and network resources. Remote users can work with files on network drives, email, intranet sites, and applications just as if they are working inside of their organization's firewall.

The Firebox SSL VPN Gateway also provides kiosk mode, which opens a virtual network computing-like connection to the Firebox SSL VPN Gateway. Kiosk mode can include shared network drives, a variety of built-in clients, servers running Windows Terminal Services (Remote Desktop), and client applications.

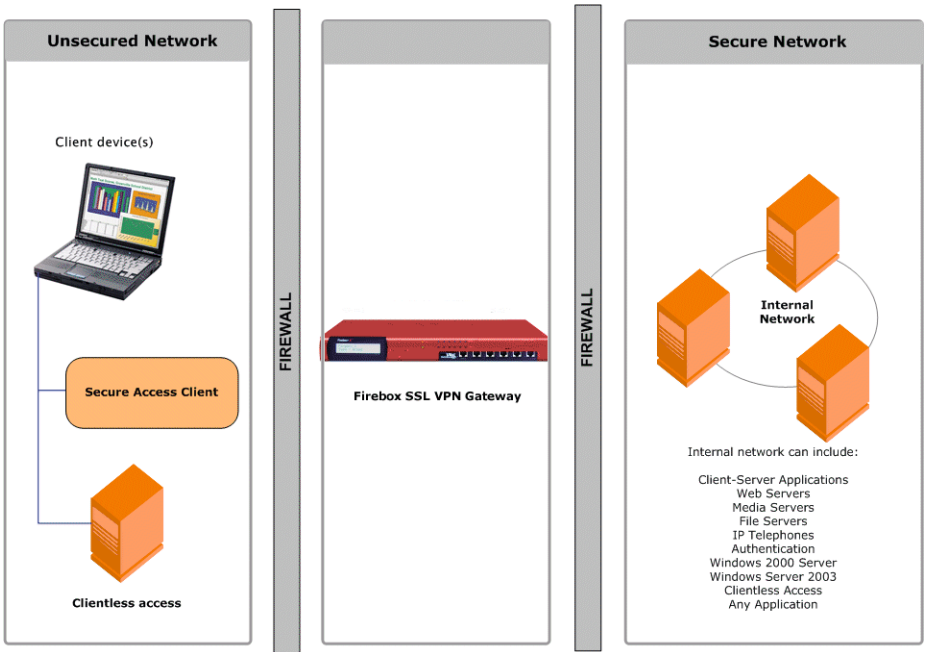
The following topics provide an overview to the Firebox SSL VPN Gateway:

- Overview
- New Features
- The User Experience
- Deployment and Administration
- Using the Firebox SSL VPN Gateway
- Using Kiosk Mode

Overview

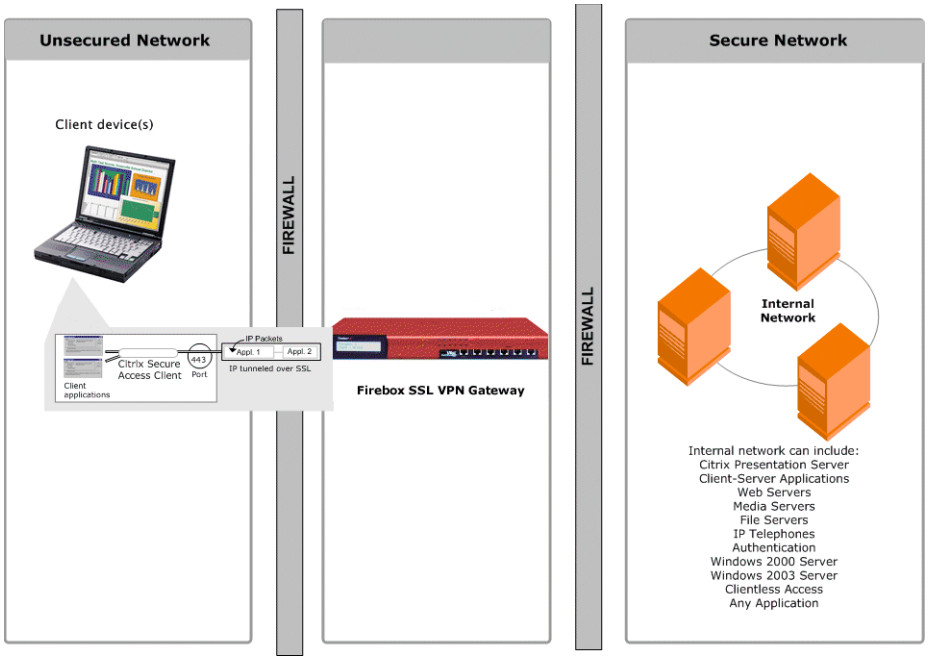
The Firebox SSL VPN Gateway is typically installed in the network demilitarized zone (DMZ) between the public and private networks. Placing the Firebox SSL VPN Gateway in front of the private network protects internal server and IT resources. The Firebox SSL VPN Gateway can also partition internal local area networks for access control and security between any two networks, such as wired/wireless and data/voice networks.

As shown in the following illustration, the Firebox SSL VPN Gateway is appropriate for employees accessing the organization remotely and intranet access from restricted LANs such as wireless networks.



Network topography showing the Firebox SSL VPN Gateway in the DMZ.

The following illustration shows how the Firebox SSL VPN Gateway creates a secure virtual TCP circuit between the client computer running the Secure Access Client and the Firebox SSL VPN Gateway.



Network topology showing the TCP circuit.

The virtual TCP circuit is using industry standard Secure Socket Layer (SSL) and Transport Layer Security (TLS) encryption. All packets destined for the private network are transported over the virtual TCP circuit. The Firebox SSL VPN Gateway is essentially acting as a low-level packet filter with encryption. It drops traffic that does not have authentication or does not have permission for a particular network.

The Firebox SSL VPN Gateway opens up the following ports:

- Port 443 is opened for VPN network traffic
- Ports 9001 and 9002 are opened for administrator traffic for the Administration Portal and Administration Tool

The first time the Firebox SSL VPN Gateway is started, use the Firebox SSL VPN Gateway Administration Tool to configure the basic settings that are specific to your corporate network, such as the IP address, subnet mask, default gateway IP address, and DNS address. After you complete the basic connection, you then configure the settings specific to Firebox SSL VPN Gateway operation, such as the options for authentication, authorization, and group-based access control, kiosk mode, end point resources and polices, portal pages, and IP pools.

New Features

The v5.5 software update for the Firebox SSL Core VPN Gateway includes the following new features:

Authentication and one-time passwords

You can configure the Firebox SSL VPN Gateway to prevent caching of one-time passwords, such as those used by an RSA SecurID. When this feature is enabled, it prevents users from being locked out of their accounts in the event of a network interruption.

New versions of the Secure Access Client

There is a new version of the Secure Access Client for Windows Vista. This version of the Secure Access Client is installed with the same ease-of-use as other versions of the Secure Access Client.

Configurable symmetric encryption ciphers

You can select the specific cipher that the Firebox SSL VPN Gateway uses for symmetric data encryption on an SSL connection. You can select one of these three encryption ciphers:

RC4 128 Bit, MD5/SHA

3DES, SHA

AES 128/256 Bit, SHA

Automatic detection of proxy server settings

In this release, the Secure Access Client automatically detects the proxy server settings specified in the operating system and when users are using Internet Explorer. Proxy server settings specified in proxy autoconfiguration files are not supported.

Secure Access Client connections

The Secure Access Client included in this release can connect to earlier versions of the Firebox SSL VPN Gateway. Also,earlier versions of the Secure Access Client can connect to this release of the Firebox SSL VPN Gateway if enabled on the **Global Cluster Policies** tab.

Automatic port redirection

You can configure the Firebox SSL VPN Gateway so that any unsecure HTTP connection attempt on port 80 is automatically redirected by the Firebox SSL VPN Gateway to a secure HTTPS connection attempt on port 443 (or other administrator-specified port).

Disable desktop sharing

You can disable the desktop sharing feature of the Secure Access Client for a user group. The Secure Access Client desktop sharing feature allows a user to view a list of all other users who are logged on. If this capability causes privacy concerns for your organization, you can disable the desktop sharing feature to prevent a specific group of users from viewing the list of online users.

Additional control over Secure Access Client connections

You can configure the Secure Access Client to disconnect from the Firebox SSL VPN Gateway if there is no user activity on the connection for a specific time interval. You can also force a client disconnection if the connection remains active for a specific time interval or if the Firebox SSL VPN Gateway does not detect keyboard or mouse activity.

Disable kiosk mode

In this release, you can disable kiosk mode for client connections. When kiosk mode is disabled, users do not see the kiosk link on the Web portal page. Users are only allowed to log on using the full Secure Access Client.

Specify multiple ports and port ranges for network resources

This release allows you to configure port ranges. You have four options when configuring the ports the Firebox SSL VPN Gateway uses to connect to internal network resources. You can specify a single port, multiple individual ports, a range of ports, or all ports.

Voice over IP softphone support

The Firebox SSL VPN Gateway supports voice over IP softphones from Avaya, Nortel, and Cisco.

Editable HOSTS file

You can edit the HOSTS file on the Firebox SSL VPN Gateway from the user interface of the Administration Tool. The Firebox SSL VPN Gateway uses the HOSTS file in conjunction with DNS servers to force DNS resolution to translate host names to IP addresses.

NTLM authentication and authorization support.

If your environment includes Windows NT 4.0 domain controllers, the Firebox SSL VPN Gateway can authenticate users against the user domain accounts maintained on the Windows NT server. The Firebox SSL VPN Gateway can also authorize users to access internal network resources based on a user's group memberships on the Windows NT 4.0 domain controller.

Added challenge-response to RADIUS user authentication

The Access Gateway now supports challenge-response token authentication with new PIN and next token modes when RSA SecurID authentication is used with RADIUS.

SafeWord PremierAccess changed to support standards-based RADIUS token user authentication

The proprietary PremierAccess configuration file has been removed and replaced using RADIUS server support. Legacy SafeWord PremierAccess realms are converted when the Firebox SSL VPN Gateway is upgraded to Version 5.5. SafeWord authentication is configured using RADIUS-style parameters.

Updated serial console menu

There are new menu items on the serial console allowing you to change the Firebox SSL VPN Gateway administrator password, set the duplex mode and network adapter speed, and revert to the default certificate that comes with the Firebox SSL VPN Gateway. Enhanced End-point and application access policies

Features

Administration Tool

The Firebox SSL VPN Gateway provides the Administration Tool to configure all of the settings for one or more Firebox SSL VPN Gateway appliances. If you have more than one Firebox SSL VPN Gateway installed, you can configure the settings once and then publish them to all of the appliances.

The Administration Tool is downloaded from the Firebox SSL VPN Gateway Administration Portal and installed on a Windows computer that is located in the secure network. A desktop icon allows you to start the Administration Tool without going to the Administration Portal.

The following sections describe the Administration Tool and where to configure the settings.

Networking, Logging, and Administration

Whether you deploy one or more appliances, basic administration of each Firebox SSL VPN Gateway is done using the **VPN Gateway Cluster** tab. This includes:

- Network configuration
- Logging
- Administration
- Statistics
- Licensing

- Date and time configuration
- Certificate generation and installation
- Restarting and shutting down the Firebox SSL VPN Gateway
- Saving and reinstalling configuration settings

Note

If the Firebox SSL VPN Gateway is upgraded to Version 5.5 from an earlier version, you must uninstall and then reinstall the latest Administration Tool. You can uninstall the earlier version of the Administration Tool using Add/Remove Programs in Control Panel.

User Groups, Local Users, and Resources

User groups, local users, and policies are configured on the **Access Policy Manager** tab. On this tab, you can configure the following:

- Network resources
- Application policies
- File sharing
- Kiosk resources
- End point resources and policies
- Local users

Authentication and Authorization

Authentication and authorization are configured on the **Authentication** tab.

Double-source authentication (also known as two-factor authentication) is new for this release of the Firebox SSL VPN Gateway.

Firebox SSL VPN Gateway Settings

The following table maps the Firebox SSL VPN Gateway settings.

Note

To configure group settings on the Access Policy Manager tab, right-click a group and then click **Properties**.

Feature	Firebox SSL VPN Gateway
General Networking	VPN Gateway Cluster > General Networking
DNS/WINS	VPN Gateway Cluster > Name Service Providers
Dynamic and Static Routing	VPN Gateway Cluster > Routes
Firebox SSL VPN Gateway Failover Servers (includes internal failover)	VPN Gateway Cluster > Failover Servers
Logging Information	VPN Gateway Cluster > Logging/Settings
Certificate Requests	VPN Gateway Cluster > Generate CSR
Certificate Installation	VPN Gateway Cluster > Administration

Feature	Firebox SSL VPN Gateway
Server Upgrade	VPN Gateway Cluster > Administration
Server Restart	VPN Gateway Cluster > Administration
Server Shut Down	VPN Gateway Cluster > Administration
Server Statistics	VPN Gateway Cluster > Statistics
Licensing	VPN Gateway Cluster > Licensing
Date and Time	VPN Gateway Cluster > Date
Enable External Administration	VPN Gateway Cluster > Administration
Saving and Restoring Server Configuration	VPN Gateway Cluster > Administration
Enable Split Tunneling	Global Cluster Policies
Accessible Networks	Global Cluster Policies
Deny Access without ACL	Global Cluster Policies
Require SSL Client Certificates	Global Cluster Policies
Validate SSL Certificates for Internal Connections	Global Cluster Policies
Improve Latency for Voice over IP Traffic	Global Cluster Policies
Internal Failover	Global Cluster Polices
Enable Portal Page Authentication	Global Cluster Policies
Configuration of Double Source Authentication	Two Source radio button
Authentication and Authorization (LDAP, RADIUS, RSA SecurID, local, and Safeword PremierAccess)	Authentication > Authentication Authentication > Authorization
Local Users	Access Policy Manager
Inherit Default Group Properties	Access Policy Manager > User Groups > Properties > General
Authentication after network interruption	Access Policy Manager > User Groups > Properties > General
Authenticate upon system resume	
Enable Single Sign-On	Access Policy Manager > User Groups > Properties > General
Run Logon Scripts	Access Policy Manager > User Groups > Properties > General
Session Time-out	Access Policy Manager > User Groups > Properties > General
Deny Applications without Policies	Access Policy Manager > User Groups > Properties > General
Enable Split DNS	Access Policy Manager > User Groups > Properties > Networking
Enable IP pools	Access Policy Manager > User Groups > Properties > Networking
Custom Portal Page	Access Policy Manager > User Groups > Properties > Gateway Portal
Web Interface Configuration (defines portal homepage and proxy server)	Access Policy Manager > User Groups > Properties > Gateway Portal
Passthrough Authentication	Access Policy Manager > User Groups > Properties > Gateway Portal

Feature	Firebox SSL VPN Gateway
Use SSL/TLS	
Local Group Users	Access Policy Manager > User Groups > Properties > Members
Client Certificate Criteria Expression	Access Policy Manager > User Groups > Properties > Client Certificates
Network Resource Groups	Access Policy Manager > Network Resources
Application Policies	Access Policy Manager > Application Policies
File Share Resources	Access Policy Manager > File Share Resources
Kiosk Resources and Policies	Access Policy Manager > Kiosk Resources
End Point Resource and Policies	Access Policy Manger > End Point Resources Access Policy Manager > End Point Policies
Pre-Authentication Policies	Access Policy Manager > Global Policies
Portal Page Configuration	Portal Page Configuration
Group Priority	Group Priority
Publish	Publish

Feature Summary

The following are key Firebox SSL VPN Gateway features:

- Universal SSL VPN. Supports all applications and protocols that improve productivity by providing users with access to the applications and resources they need, without the need for customization or converting the content for Web access.
- Standards-based security. Information is kept private and protected using industry standard SSL/TLS encryption. Users are authenticated using standards such as LDAP, RADIUS, double-source authentication, and client and server certificates.
- Web-deployed client. There is no need to preinstall or manage complex client software, reducing the cost of ownership. (Note that a user must have Administrator access on the Windows computer to install the client from the Web).
- Desk-like access. Users receive the same network experience and application access as if physically connected to the corporate network.
- Always-on access. Automatically reconnects users to the appliance as soon as the network connection is restored. Reduces user frustration when using public networks, such as wireless connections in hotels or airports.
- Integrated end-point scanning. Ensures that the computer meets corporate standards to connect and remains safe for connection to the network.
- Hides internal IP addresses. There is no IP stack or routing table entry, so internal IP addresses are hidden, reducing the threat of worms propagating.

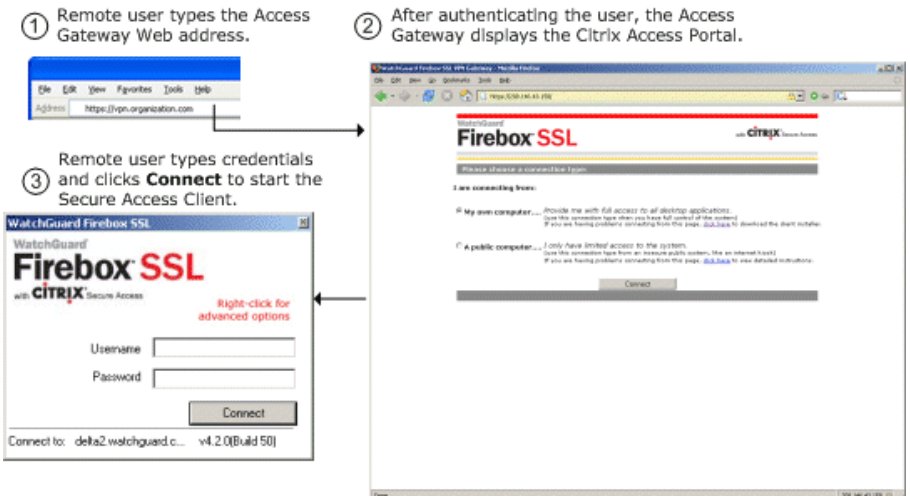
The User Experience

The Firebox SSL VPN Gateway provides users with the desk-like network experience that they have with an IPSec VPN, but does so without any need to pre-install or configure a client. The user starts the

Secure Access Client by typing a secure Web address in a standard Web browser and providing authentication credentials.

Because the Firebox SSL VPN Gateway encrypts traffic using standard SSL/TLS, it can traverse firewalls and proxy servers, regardless of the client location. For a more detailed description of the user experience, see “Connecting from a Private Computer” on page 119.

The following illustration shows the Windows version of the Access Portal.



Connecting to the Firebox SSL Access Portal.

Note

The Firebox SSL Access Portal can be customized. For more information, see “Using Portal Pages” on page 38. You can also include a link to the clients on a Web site. For more information, see “Linking to Clients from Your Web Site” on page 41.

After a successful logon, the user can work with network shares and use applications just as if the user were sitting in the office.

Deployment and Administration

The Firebox SSL VPN Gateway is quick and easy to deploy and simple to administer. The most typical deployment configuration is to locate the Firebox SSL VPN Gateway behind your firewall or in the demilitarized zone (DMZ). More complex deployments, such as with a server load balancer, are also supported and described in this chapter.

The first time the Firebox SSL VPN Gateway is started, use the Firebox SSL VPN Gateway Administration Tool to configure the basic settings that are specific to your corporate network, such as the Firebox SSL VPN Gateway IP address, subnet mask, default gateway IP address, and DNS address. After you complete the basic connection, you then configure the settings specific to Firebox SSL VPN Gateway operation, such as the options for authentication, authorization, and group-based access control; kiosk mode, end point resources and polices, portal pages, and IP pools.

Firebox SSL VPN Gateway monitoring is performed through the Firebox SSL VPN Gateway Administration Desktop, providing access to a variety of standard network monitoring tools, including Ethereal Network Monitor, xNetTools, Traceroute, fnetload, and System Monitor. The Firebox SSL VPN Gateway

Administration Desktop also provides access to the Real-Time Monitor, where you can view a list of current users and close the connection for any user.

Planning your deployment

This chapter discusses deployment scenarios for the Firebox SSL VPN Gateway. You can deploy the Firebox SSL VPN Gateway at the perimeter of your organization's internal network (or intranet) to provide a secure single point-of-access to the servers, applications, and other network resources residing in the internal network. All remote users must connect to the Firebox SSL VPN Gateway before they can access any resources on the internal network.

This section discusses the following Firebox SSL VPN Gateway deployments:

- Deploying the Firebox SSL VPN Gateway in the network demilitarized zone (DMZ)
- Deploying the Firebox SSL VPN Gateway in a secure network that does not have a DMZ

Deploying the Firebox SSL VPN Gateway in the Network DMZ

Many organizations protect their internal network with a DMZ. A DMZ is a subnet that lies between an organization's secure internal network and the Internet (or any external network). When the Firebox SSL VPN Gateway is deployed in the DMZ, users access it using the Secure Access Client or the kiosk client.

In this configuration, you install the Firebox SSL VPN Gateway in the DMZ and configure it to connect to both the Internet and the internal network. When you deploy the Firebox SSL VPN Gateway in the DMZ, client connections must traverse the first firewall to connect to the Firebox SSL VPN Gateway. By default, clients use Secure Sockets Layer (SSL) on port 443 to establish this connection. To support this connectivity, you must allow SSL on port 443 through the first firewall.

Note

You can change the port clients use to connect to the Firebox SSL VPN Gateway by altering the port setting in the Administration Tool. This port setting is discussed in "Configuring TCP/IP Settings Using Network Cables".

. The Firebox SSL VPN Gateway decrypts the SSL connections from the client and establishes a connection on behalf of the client to the network resources behind the second firewall. The ports that must be open through the second firewall are dependent on the network resources that you authorize external users to access.

For example, if you authorize external users to access a Web server in the internal network, and this server listens for HTTP connections on port 80, you must allow HTTP on port 80 through the second firewall. The Firebox SSL VPN Gateway establishes the connection through the second firewall to the HTTP server on the internal network on behalf of the external clients.

The Firebox SSL VPN Gateway administrative tools available on the Firebox SSL VPN Gateway also listen for connections on these ports:

- Port 9001 - Connections to the Administration Portal occur on this port.
- Port 9002 - Connections to the Administration Tool occur on this port

Deploying the Firebox SSL VPN Gateway in a Secure Network

You can install the Firebox SSL VPN Gateway in the secure network. In this scenario, there is typically one firewall between the Internet and the secure network. The Firebox SSL VPN Gateway resides inside the firewall to control access to the network resources.

When an Firebox SSL VPN Gateway is deployed in the secure network, the Secure Access Client or kiosk client connections must traverse the firewall to connect to the Firebox SSL VPN Gateway. By default, both of these clients use the SSL protocol on port 443 to establish this connection. To support this connectivity, you must open port 443 on the firewall.

Note

You can change the port on which clients connect to the Firebox SSL VPN Gateway by altering the port setting in the Administration Tool. This port setting is discussed in "Configuring TCP/IP Settings Using Network Cables".

Planning for Security with the Firebox SSL VPN Gateway

When planning any type of Firebox SSL VPN Gateway deployment, there are basic security issues associated with certificates, authentication, and authorization that you should understand.

Configuring Secure Certificate Management

By default, the Firebox SSL VPN Gateway includes a self-signed SSL server certificate that enables it to complete SSL handshakes. Self-signed certificates are adequate for testing or sample deployments, but are not recommended for production environments.

Before you deploy the Firebox SSL VPN Gateway in a production environment, WatchGuard recommends that you request and receive a signed SSL server certificate from a known Certificate Authority and upload it to the Firebox SSL VPN Gateway.

If you deploy the Firebox SSL VPN Gateway in any environment where the Firebox SSL VPN Gateway must operate as the client in an SSL handshake (initiate encrypted connections with another server), you must also install a trusted root certificate on the Firebox SSL VPN Gateway. For more information about root certificates, see "Installing Root Certificates on the Firebox SSL VPN Gateway" on page 112.

For more information about certificates, see "Creating and Installing Secure Certificates" on page 109.

Authentication Support

You can configure the Firebox SSL VPN Gateway to authenticate users and control the level of access (or authorization) that users have to the network resources on the internal network.

Before deploying the Firebox SSL VPN Gateway, your network environment should have the corporate directories and authentication servers in place to support one of these authentication types:

- LDAP
- RADIUS
- RSA SecurID
- NTLM
- Secure Computing SafeWord products

If your environment supports none of the authentication types listed above, or you have a small population of remote users, you can create a list of local users on the Firebox SSL VPN Gateway and configure the Firebox SSL VPN Gateway to authenticate users against this local list. With this configuration, it is not necessary to maintain user accounts in a separate, external directory.

For more information about authentication and authorization, see "Configuring Authentication and Authorization" on page 61.

Deploying Additional Appliances for Load Balancing and Failover

You can install multiple Firebox SSL VPN Gateway appliances into your environment for one or both of these reasons:

- **Scalability.** If you have a large remote user population, install additional Firebox SSL VPN Gateway appliances to accommodate the user load.
- **High Availability.** If an Firebox SSL VPN Gateway fails, you can install an additional Firebox SSL VPN Gateway to ensure that the internal network remains available to remote users.

Note

To support only high availability, you can configure one Firebox SSL VPN Gateway as the primary Firebox SSL VPN Gateway and one (or more) Firebox SSL VPN Gateway appliances as a failover device. If the primary Firebox SSL VPN Gateway fails, client connections are directed to the failover Firebox SSL VPN Gateway. For more information about this configuration, see "Configuring Firebox SSL VPN Gateway Failover" on page 55.

To support both scalability and high availability, you can install a load balancer and then install multiple Firebox SSL VPN Gateway appliances behind the load balancer. Deploying multiple appliances behind a load balancer enables you to support a large population of remote users and maintain high availability of the internal network to the users.

Installing the Firebox SSL VPN Gateway for the First Time

The Firebox SSL VPN Gateway installs in any network infrastructure without requiring changes to the existing hardware or back-end software. It works with other networking products such as cache engines, firewalls, routers, and IEEE 802.11 wireless devices.

WatchGuard recommends installing the Firebox SSL VPN Gateway in the corporate demilitarized zone (DMZ). When installed in the DMZ, the Firebox SSL VPN Gateway participates on two networks: a private network and a public network with a publicly routable IP address. Typically, the private network is the corporate network and the public one is the Internet. You can also use the Firebox SSL VPN Gateway to partition local area networks internally in the organization for access control and security. You can create partitions between wired or wireless networks and data and voice networks.

Getting Ready to Install the Firebox SSL VPN Gateway

Before installing the Firebox SSL VPN Gateway, collect materials for the initial configuration and for the connection to your network.

For initial configuration, use **one** of the following setups:

- A cross-over cable and a Windows computer
- Two network cables, a network switch, and a Windows computer
- A serial cable and a computer with terminal emulation software

For a connection to a local area network, use the following items:

- One network cable to connect the Firebox SSL VPN Gateway inside of a firewall.
- Two network cables to connect the Firebox SSL VPN Gateway located in the demilitarized zone (DMZ) to the Internet and private networks

Collect the following network information for appliances:

- The Firebox SSL VPN Gateway internal IP address and subnet mask
- The Firebox SSL VPN Gateway external IP address and subnet mask

- The Firebox SSL VPN Gateway FQDN for network address translation (NAT)
- The IP address of the default gateway device
- The port to be used for connections

If connecting the Firebox SSL VPN Gateway to a server load balancer:

- The Firebox SSL VPN Gateway IP address and subnet mask.
- The settings of the server load balancer as the default gateway device (if required). See the load balancer manufacturer's documentation for more information.
- The FQDN of the server load balancer to be used as the external public address of the Firebox SSL VPN Gateway.
- The port to be used for connections.

Note

The Firebox SSL VPN Gateway does not work with Dynamic Host Configuration Protocol (DHCP). The Firebox SSL VPN Gateway requires the use of static IP addresses.

Setting Up the Firebox SSL VPN Gateway Hardware

This section provides procedures for setting up the Firebox SSL VPN Gateway for the first time.

To physically connect the Firebox SSL VPN Gateway

1 Install the Firebox SSL VPN Gateway in a rack if it is rack-mounted.

2 Connect the power cord to the AC power receptacle.

3 Connect either the serial cable to a Windows computer, a cross-over cable to a Windows computer, or an RJ-45 network cable to a network switch and the Access Gateway.

4 Configure the TCP/IP settings using the instructions in "Configuring TCP/IP Settings for the Firebox SSL VPN Gateway"

Configuring TCP/IP Settings for the Firebox SSL VPN Gateway

The preconfigured IP address of the Firebox SSL VPN Gateway is 10.20.30.40. The IP address can be changed using a serial cable and a terminal emulation program, or by connecting the Firebox SSL VPN Gateway using network cables and the Administration Tool.

You can use the serial console to set the IP address and subnet of the Firebox SSL VPN Gateway Interface 0, as well as the IP address of the default gateway device. All other configuration must be done using the Administration Tool. You can also use the serial console to test a connection with the ping command. If you want to reach the Firebox SSL VPN Gateway through the serial console before making any configuration settings, use a serial cable to connect the Firebox SSL VPN Gateway to a computer that has terminal emulation software.

The serial console provides the following options for configuring the Firebox SSL VPN Gateway:

- **[0] Express Setup** configures the TCP/IP settings for Interface 0 on the **Firebox SSL VPN Gateway Cluster > General Networking** tab
- **[1] Ping** is used to ping other network devices to check for connectivity
- **[2] Link Modes** is used to set the duplex mode and speed mode for Interface 0 on the **Firebox SSL VPN Gateway Cluster > General Networking** tab
- **[3] External Administration Port** enables or disables connections to the Administration Tool from a remote computer

- **[4] Display Log** displays the Firebox SSL VPN Gateway log
- **[5] Reset Certificate** resets the certificate to the default certificate that comes with the Firebox SSL VPN Gateway
- **[6] Change Administrative Password** allows you to change the default administrator password of **rootadmin**

Note

Important: WatchGuard recommends changing the administrator password before connecting the Firebox SSL VPN Gateway to your network. The new password can be six to 127 characters long and cannot begin or end with a space.

- **[7] Help** displays help information
- **[8] Log Out** logs off from the Firebox SSL VPN Gateway

Note

WatchGuard recommends using both network adapters on the appliance. After configuring the TCP/IP settings for Interface 0, use the Administration Tool to configure TCP/IP settings for Interface 1.

To configure TCP/IP settings using a serial cable

1 Connect the serial cable to the 9-pin serial port on the Firebox SSL VPN and connect the cable to a computer that is capable of running terminal emulation software.

2 On the computer, start a terminal emulation application such as HyperTerminal.

Note

HyperTerminal is not automatically installed on Windows 2000 Server or Windows Server 2003. To install HyperTerminal, use Add/Remove Programs in the Control Panel.

3 Set the serial connection to 9600 bits per second, 8 data bits, no parity, 1 stop bit. Hardware flow control is optional.

4 Turn on the Firebox SSL VPN. The serial console appears on the computer terminal after about three minutes.

5 If using HyperTerminal, press the **Enter** key.

6 On the serial console, enter the default administrator credentials. The user name is **root** and the password is **rootadmin**.

Note

Important: Watchguard recommends changing the administrator password. You can do this using the Administration Portal or the serial console.

7 To set the IP address and subnet mask and the default gateway device for Interface 0, type **0** and press **Enter** to choose Express Setup. After you respond to the prompts, the information you entered appears. To commit your changes, type **y**; the Access Gateway restarts.

8 To verify that the Firebox SSL VPN can ping a connected network device, type **1** and enter the IP address of the device.

9 Remove the serial cable and connect the Firebox SSL VPN using either a cross-over cable to a Windows computer or a network cable to a network switch and then turn on the Firebox SSL VPN.

Additional Firebox SSL VPN settings are configured using the Administration Tool.

To configure TCP/IP Settings Using Network Cables

The Firebox SSL VPN Gateway has two network adapters installed. One network adapter communicates with the Internet and client computers that are not inside the corporate network. The other network adapter communicates with the internal network.

WatchGuard recommends that both network adapters be configured for maximum security. If only one network adapter is used, it has to be routable for internal resources using Network Address Translation (NAT). Also, if only one network adapter is used, throughput of network traffic is cut in half and can cause a bottleneck of network traffic.

You can install the Firebox SSL VPN Gateway and configure TCP/IP settings using network cables, such as two RJ-45 network cables, or cross-over cables. The RJ-45 cables are connected to a network switch and to the Firebox SSL VPN Gateway. The cross-over cables are connected to a Windows computer and the Firebox SSL VPN Gateway.

To configure TCP/IP settings using network cables

1 Power on the Firebox SSL VPN Gateway.
After about three minutes, the Firebox SSL VPN Gateway is ready for its initial configuration with your network.

2 Open a Web browser and type https://10.20.30.40:9001 to open the Administration Portal. Use the default user name and password of **root** and **rootadmin**.

3 On the **Downloads** tab, under **Firebox SSL VPN Gateway Administration Tool**, click **Install the Firebox SSL VPN Gateway Administration Tool**.
Follow the prompts to complete installation.

4 Log on to the Administration Tool using the default user name and password.

5 On the **Firebox SSL VPN Gateway Cluster** tab, open the window for the Firebox SSL VPN Gateway.

6 On the **General Networking** tab, under **Interface 0** and **Interface 1**, next to **IP Address**, type the new IP addresses of the appliance.

7 In **Subnet mask**, enter the subnet mask that is appropriate for the IP address entered for the interface(s).

8 In **External FQDN**, type the fully qualified domain name.

Note

Important: The FQDN must match what is on the digital certificate and the license for the Firebox SSL VPN Gateway.

9 In **Duplex Mode** select the direction of the transmission data. The default setting is **auto**. You can also select full duplex or half duplex.

10 In **Speed Mode** select the network speed of the adapter.
The default setting is auto. You can also select 10Mbps, 100Mbps, or 1000Mbps.

11 In **Maximum Transmission Unit (MTU)**, select the maximum transmission unit that defines the maximum size of the transmitted packet.
The default setting is 1500.

12 In **Port**, select the incoming port that is used for connections. The default is 443.

13 To configure a default gateway, in **IP address**, type the IP address of the gateway. In **Interface**, select the network adapter on the Firebox SSL VPN Gateway with which the Default Gateway communicates.

The IP address is the default gateway device, such as the main router, firewall, or server load balancers, depending on your network configuration. This should be the same as the Default Gateway setting that is on computers on the same subnet.

For information about the relationship between the Default Gateway and dynamic or static routing, see "Dynamic and Static Routing" on page 51.

After you configure your network settings on the Firebox SSL VPN Gateway, you need to restart the appliance.

Note

Note: You do not need to restart the Firebox SSL VPN Gateway until you complete all configuration steps.These include configuring network access for the appliance and installing certificates and licenses. For more information about configuring additional network settings, see"Configuring Firebox SSL VPN Gateway Network Connections" on page 47.

Redirecting Connections on Port 80 to a Secure Port

By default, the Firebox SSL VPN Gateway does not accept unsecure connections on port 80. If a user attempts to connect to the Firebox SSL VPN Gateway using HTTP on port 80, the connection attempt fails.

You can configure the Firebox SSL VPN Gateway to automatically redirect HTTP connection attempts on port 80 to be secure connections on port 443 (or other secure port).

If a user attempts an unsecure connection on port 80, the Firebox SSL VPN Gateway automatically converts this connection attempt into a secure (SSL-encrypted) connection on port 443.

To redirect unsecure connections

1 Click the **Firebox SSL VPN Gateway Cluster** tab and open the window for the Firebox SSL VPN Gateway.

2 Click the **General Networking** tab.

3 Click the **Advanced** button.

4 Click **Redirect any requests for port 80 to a secure port**.

5 Click **OK**.

Note

Note: If you use the default setting of **Do not accept connections on port 80**, all user connection attempts on port 80 fail and there is no attempt to redirect them to port 443.

Using the Firebox SSL VPN Gateway

The Firebox SSL VPN Gateway performs the following functions:

- Authentication
- Termination of encrypted sessions
- Access control (based on permissions)
- Data traffic relay (when the first three functions are met)

The Firebox SSL VPN Gateway operates as follows:

- A remote user downloads the Secure Access Client by connecting to a secure Web address and providing authentication credentials.

- After downloading the Secure Access Client, the user logs on. When the user successfully authenticates, the Firebox SSL VPN Gateway establishes a secure tunnel.
- As the remote user attempts to access network resources across the VPN tunnel, the Secure Access Client encrypts all network traffic destined for the organization's intranet and forwards the packets to the Firebox SSL VPN Gateway.
- The Firebox SSL VPN Gateway terminates the SSL tunnel, accepts any incoming traffic destined for the private network, and forwards the traffic to the private network. The Firebox SSL VPN Gateway sends traffic back to the remote computer over a secure tunnel.

Starting the Secure Access Client

A remote user installs the Secure Access Client by typing a secure Web address, typically the fully qualified domain name (FQDN) of the Firebox SSL VPN Gateway. The Firebox SSL VPN Gateway prompts the user for authentication over HTTP 401 Basic or Digest. The Firebox SSL VPN Gateway authenticates the credentials using one of the following authentication methods: local authentication, RSA SecureID, SafeWord PremierAccess, LDAP, or RADIUS. If the credentials are correct, the Firebox SSL VPN Gateway finishes the handshake with the client. This logon step is required only when a user initially downloads the Secure Access Client.

If the user is behind a proxy server, the user can specify the proxy server's IP address and authentication credentials.

To configure a proxy server

1 To open the logon dialog box, click the Secure Access Client icon on the desktop.

2 In the **Firebox SSL Secure Access** logon dialog box, right-click anywhere in the dialog box and select **Advanced Options**.

3 In the **Firebox SSL Secure Access Options** dialog box, under **Proxy Settings**, select **Use Proxy Host**.

4 In **Proxy Address** and **Proxy Port**, type the IP address and port number.

5 If the authentication is required by the server, select **Proxy server requires authentication**.

The Secure Access Client is installed on the user's computer. After the first connection, the remote user can subsequently use a desktop shortcut to start the Secure Access Client.

The Advanced Options dialog box can also be opened by right-clicking the Firebox SSL Secure Access icon on the desktop and then clicking **Properties**.

Enabling Single Sign-On Operation for the Secure Access Client

If the Secure Access Client is configured for single sign-on operation, it automatically starts after the user logs on to Windows. The user's Windows logon credentials are passed to the Firebox SSL VPN Gateway for authentication. Enabling single sign-on for the Secure Access Client facilitates operations on the remote computer such as installation scripts and automatic drive mapping.

For more information about configuring single sign-on, see "Configuring Secure Access Client for single sign-on" on page 91.

Note

Users must be logged on as a local administrator or be a member of the Administrators group to use single sign-on for Secure Access Client.

Establishing the Secure Tunnel

After the Secure Access Client is started, it establishes a secure tunnel over port 443 (or any configured port on the Firebox SSL VPN Gateway) and sends authentication information. When the tunnel is established, the Firebox SSL VPN Gateway sends configuration information to the Secure Access Client describing the networks to be secured and containing an IP address if you enabled IP pool visibility.

Tunneling Destination Private Address Traffic over SSL or TLS

After the Secure Access Client is authenticated and started, all network traffic destined for specified private networks is captured and redirected over the secure tunnel to the Firebox SSL VPN Gateway.

The Firebox SSL VPN Gateway intercepts connections that are to be tunneled (usually trafic to your according to your policy, and multiplexes/tunnels them over SSL to the Firebox SSL VPN Gateway. where the traffic is demultiplexed and the connections are forwarded to the correct host and port combination.

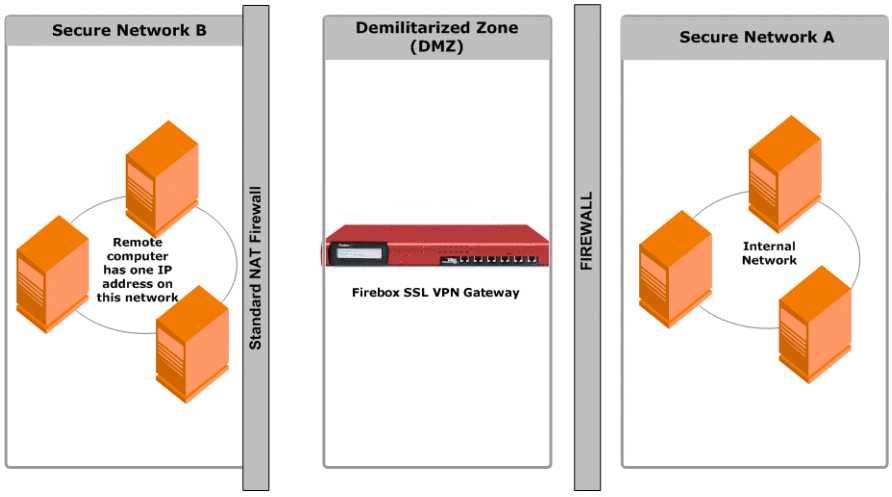
The connections are subject to administrative security policies that apply to a single application, a subset of applications, or an entire intranet. You use the Firebox SSL VPN Gateway Administration Tool to specify the resources (ranges of IP address/subnet pairs) that remote users can access through the VPN connection.

If the device is configured todo this, all IP packets, regardless of protocol, are intercepted and transmitted over the secure link. Connections from local applications on the client computer are securely tunneled to the Firebox SSL VPN Gateway, which reestablishes the connections to the target server. Target servers view connections as originating from the local Firebox SSL VPN Gateway on the private network, thus hiding the client IP address. This is also called *reverse Network Address Translation* (NAT). Hiding IP addresses adds security to source locations.

Locally, on the client computer, all connection-related traffic (such as SYN-ACK, PUSH, ACK, and FIN packets) are recreated by the Secure Access Client to appear from the private server.

Operation through Firewalls and Proxies

Users of Secure Access Client are sometimes located inside of another organization's firewall, as shown in the following illustration.



Network topology connecting through an external corporate firewall.

NAT firewalls maintain a table that allows them to route secure packets from the Firebox SSL VPN Gateway back to the client computer. For circuit-oriented connections, the Firebox SSL VPN Gateway maintains a port-mapped, reverse NAT translation table. The reverse NAT translation table enables the Firebox SSL VPN Gateway to match connections and send packets back over the tunnel to the client with the correct port numbers so that the packets return to the correct application.

The Firebox SSL VPN Gateway tunnel is established using industry-standard connection establishment techniques such as HTTPS, Proxy HTTPS, and SOCKS. This operation makes the Firebox SSL VPN Gateway firewall friendly and allows remote computers to access private networks from behind other organizations' firewalls without creating any problems.

For example, the connection can be made through an intermediate proxy, such as an HTTP proxy, by issuing a CONNECT HTTPS command to the intermediate proxy. Any credentials requested by the intermediate proxy, are in turn obtained from the remote user (by using single sign-on information or by requesting the information from the remote user) and presented to the intermediate proxy server. When the HTTPS session is established, the payload of the session is encrypted and carries secure packets to the Firebox SSL VPN Gateway.

Terminating the Secure Tunnel and Returning Packets to the Client

The Firebox SSL VPN Gateway terminates the SSL tunnel and accepts any incoming packets destined for the private network. If the packets meet the authorization and access control criteria, the Firebox SSL VPN Gateway regenerates the packet IP headers so that they appear to originate from the Firebox SSL VPN Gateway's private network IP address range or the client-assigned private IP address. The Firebox SSL VPN Gateway then transmits the packets to the network.

Note

If you run a packet sniffer such as Ethereal on the computer where the Secure Access Client is running, you will see unencrypted traffic that appears to be between the client and the Firebox SSL VPN Gateway. That unencrypted traffic, however, is not over the tunnel between the client and the Firebox SSL VPN Gateway but rather the tunnel to the local applications.

The Secure Access Client maintains two tunnels: an SSL tunnel over which data is sent to the Firebox SSL VPN Gateway (the sniffer also detects this tunnel) and a tunnel between the client and local applications. The encrypted data that arrives over the SSL tunnel is then decrypted before being sent to the local application over the second tunnel. The packet sniffer sees the second tunnel's traffic, which appears to be from the Firebox SSL VPN Gateway, after the traffic is already decrypted.

When an application client connects to its application server, certain protocols may require that the application server in turn attempt to create a new connection with the client. In this case, the client sends its known local IP address to the server by means of a custom client-server protocol. For these applications, the Secure Access Client provides the local client application a private IP address representation, which the Firebox SSL VPN Gateway uses on the internal network. Many real-time voice applications and FTP use this feature.

Performance and Real-Time Traffic

Real-time applications, such as voice and video, are implemented over UDP, because TCP is not appropriate for real-time traffic due to the delay introduced by acknowledgements and retransmission of lost packets. It is more important to deliver packets in real time than to ensure that all packets are delivered. However, with any tunneling technology over TCP, such real-time performances cannot be met.

The Firebox SSL VPN Gateway overcomes this issue by routing UDP packets over the secure tunnel as special IP packets that do not require TCP acknowledgements. Even if the packets get lost in the net-

work, no attempt is made by either the client or the server applications to regenerate them, so real-time (UDP like) performance is achieved over a secure TCP-based tunnel.

For more information about improving latency with UDP connections and Voice over IP, see "Improving Voice over IP Connections" on page 59.

Using Kiosk Mode

The Firebox SSL VPN Gateway provides secure access to a corporate network from a public computer using kiosk mode. When users select **A public computer** on the Firebox SSL Access Portal page, the Web browser opens. The user logs on and then can access applications provided in the browser window.

- For computers running Windows 2000 and above, kiosk mode is available through the Access Portal. The link can be removed from the Access Portal on a group basis.
- For computers running JVM 1.5 or higher (such as Macintosh, Windows 95, or Windows 98 computers), kiosk mode is available through a Java applet. For Macintosh, Safari is the supported browser.

When the user is logged on using kiosk mode, the Firebox SSL VPN Gateway sends images only (no data) over the connection. As a result, there is no risk of leaving temporary files or cookies on the public computer. Both temporary files and cookies are maintained on the Firebox SSL VPN Gateway for the session.

The browser defaults to a Web address that is configured per group through the Firebox SSL VPN Gateway Administration Tool. The Web browser window can also include icons for Remote Desktop, SSH, Telnet 3270 emulator, Gaim instant messenging, and VNC clients. The icons are displayed in the bottom-left corner of the window. The applications are specified for each group. For more information about configuring applications for kiosk mode, see "Configuring kiosk mode" on page 103.

The Web browser window also provides access to shared network drives. The Firebox SSL VPN Gateway administrator configures the permissions granted (read-only or read/write) to each shared network drive. For more information about configuring network shares, see "Configuring file share resources" on page 102.

Users can copy files from the network share to their computer simply by dragging the file onto the KioskFTP icon and selecting the destination in the File Download dialog box.

Note

End point policies are not supported or enforced when users are logged on using kiosk mode.

Connecting to a Server Load Balancer

You can connect one or more Firebox SSL VPN Gateways to a server load balancer. Characteristics of this configuration include the following:

- Incoming Web traffic is intercepted by the server load balancer and load balanced among multiple Firebox SSL VPN Gateways.
- For optimal load balancing, configure the settings to balance connections based on SSL session identifiers (IDs). Load balancing based on source IP (Src IP) is also supported.
- For optimal performance, the server load balancer is configured with a fully qualified domain name (FQDN). The FQDN is used by the Firebox SSL VPN Gateway when reestablishing a connection to the server load balancer.
- The Firebox SSL VPN Gateway external public address is the external-facing (public) FQDN of the server load balancer. The Firebox SSL VPN Gateway modifies all requests to include the external

public address. The external public address ensures that the redirected client returns to the Firebox SSL VPN Gateway it first encountered, providing session stickiness. The association between a particular request and the Firebox SSL VPN Gateway is broken only when the client makes a new connection. To configure the Firebox SSL VPN Gateway to connect to the network, see "Configuring Network Information" on page 47.

To establish the physical connection, connect the Firebox SSL VPN Gateway eth0 interface to the internal network. Use the Firebox SSL VPN Gateway Administration Tool to configure network settings. Specify the IP address of the server load balancer as the default gateway on the Firebox SSL VPN Gateway **VPN Gateway Cluster > General Networking** tab.

Note

SSL sessions must terminate at the Firebox SSL VPN Gateway. In-line SSL acceleration hardware appliances and bridging proxy servers cannot be used.

CHAPTER 3

Configuring Basic Settings

This chapter describes Firebox SSL VPN Gateway basic administration, including connecting to the Firebox SSL VPN Gateway, using the Administration Desktop, and using the Administration Tool to configure the Firebox SSL VPN Gateway.

Note

All submitted configuration changes are applied automatically to the Firebox SSL VPN Gateway and do not cause a disruption for users connected to the Firebox SSL VPN Gateway. Policy changes take effect immediately; if a connection violates a new policy, it is closed.

Topics covered in this chapter include:

- Firebox SSL VPN Gateway Administration Desktop
- Using the Administration Tool
- Using the Administration Portal
- Using the Serial Console
- Product Activation and Licensing
- Managing Licenses
- Blocking External Access to the Administration Portal
- Using Portal Pages
- Linking to Clients from Your Web Site
- Saving and Restoring the Configuration
- Restarting the Firebox SSL VPN Gateway
- Restarting the Firebox SSL VPN Gateway
- Shutting Down the Firebox SSL VPN Gateway
- Firebox SSL VPN Gateway System Date and Time

Note

This chapter assumes that you set up the Firebox SSL VPN Gateway hardware and performed the initial configuration as described in “Getting Started with Firebox SSL VPN Gateway.”.

Firebox SSL VPN Gateway Administration Desktop

The Firebox SSL VPN Gateway Administration Desktop provides Firebox SSL VPN Gateway monitoring tools. The taskbar includes one-click access to a variety of standard Linux monitoring applications as well as the Real-Time Monitor, used to view and manage open connections, and the system time and date.

The Administration Desktop includes features for monitoring, including the Real-Time Monitor, and icons for monitoring applications. The middle of the taskbar has buttons for switching the work space and task bar buttons. The right side of the taskbar contains processor and network usage information and displays the system time and date.

The Administration Desktop is opened from the Administration Portal.

To open the Administration Portal and Administrative Desktop

1 Make sure that the Firebox SSL VPN Gateway is running.

2 From a Web browser, connect to the Firebox SSL VPN Gateway by entering the Web address:
https://*ipAddress:*9001
where:
ipAddress is the IP address of your Firebox SSL VPN Gateway.
9001 is the administration port of your Firebox SSL VPN Gateway.

3 If a **Security Alert** dialog box appears, click **Yes**.

4 Type the user name and password. The defaults are **root** and **rootadmin**.

5 The Firebox SSL VPN Gateway Administration Portal appears.

6 Click **Launch Firebox SSL VPN Gateway Administrative Desktop**.

7 In the **WatchGuard Firebox SSL Remote Admin Terminal** dialog box, type your user name and password.

Note

By default, if you configure the Firebox SSL VPN Gateway to use both network adapters, the Administration Portal can be accessed from either adapter. To block administrative access from the network adapter that connects externally, see "Blocking External Access to the Administration Portal" on page 38.

Using the Administration Portal

The Administration Portal provides a Web-based interface for administrators. There are several tabs in the Administration Portal that provide a convenient place to do some administrative tasks of the Firebox SSL VPN Gateway.

Downloads Tab

On this tab, you can do the following:

- Download the Administration Tool
- Download and install, or start, the Administration Desktop
- Download the Firebox SSL VPN Gateway Documentation
- Download portal page templates

- Download a sample email for users

Admin Users Tab

The Firebox SSL VPN Gateway has a default administrative user account with full access to the Firebox SSL VPN Gateway. To protect the Firebox SSL VPN Gateway from unauthorized access, change the default password during your initial configuration.

Note

To reset the root administrative password to its default, you must reinstall the Firebox SSL VPN Gateway server software.

The Firebox SSL VPN Gateway is preconfigured with the default user name of **root** and password of **rootadmin**.

To change the administrator password

1 In the Firebox SSL VPN Gateway Administration Portal, on the **Administration** tab, click **Admin Users**.

2 Under **Administrator Password**, type the new password in the fields provided.

3 Click **Change Password**.

Logging Tab

This tab displays the log for the Firebox SSL VPN Gateway. This is the same log that is in the Administration Tool on the **VPN Gateway Cluster > Logging** tab.

Maintenance Tab

This tab provides you a place to do administrative tasks. These are:

- Uploading a signed certificate
- Uploading a private key and certificate
- Uploading a saved configuration or appliance upgrade
- Saving the appliance configuration
- Restarting and shutting down the appliance

You can also log off from the Administration Portal by clicking **Log Out**.

Using the Serial Console

You can use the serial console to set the IP address and subnet of the Firebox SSL VPN Gateway Interface 0, as well as the IP address of the default gateway device. All other configuration must be done using the Administration Tool. You can also use the serial console to test a connection with the ping command.

If you want to reach the Firebox SSL VPN Gateway through the serial console before making any configuration settings, use a serial cable to connect the Firebox SSL VPN Gateway to a computer that has terminal emulation software.

To open the serial console

1 Connect the RS232 cable to the serial port on the Firebox SSL VPN Gateway and to the serial port on the computer.

2 Make sure that the Firebox SSL VPN Gateway is running.

3 Start a terminal emulation application (such as HyperTerminal or Putty) and create the following settings:

If the serial console does not open, check the settings in the terminal emulation application. Set the serial connection to 115,200 bits per second, 8 data bits, no parity, and 1 stop bit. The flow control should be hardware. Set the terminal emulation to ANSI or Auto. Set the application to send a delete operation when the backspace key is depressed.

4 Press **Enter** twice in the terminal emulation application. The Firebox SSL VPN Gateway Banner appears, along with the logon prompt.

5 Enter the default administrative user name **root** and password **rootadmin**.
The Serial Console menu appears.

Using the Administration Tool

The Administration Tool contains all Firebox SSL VPN Gateway configuration controls, except for administrative user account management, which is available only from the Administration Portal.

The Administration Tool allows you to configure global settings once and then publish them to multiple Firebox SSL VPN Gateways on your network.

The left pane of the Administration Tool window displays Help information for the current tab. The online Help corresponds to the task you are completing.

The Administration Tool is downloaded and installed from the Administration Portal. You can also download documentation, portal page templates, and a sample email that can be customized with instructions for users.

Note

If you upgraded from a previous version of the Firebox SSL VPN Gateway, you must uninstall the Administration Tool using Add/Remove Programs in Control Panel and then install the latest version from the Administration Portal.

To download and install the Administration Tool

1 In the Firebox SSL VPN Gateway Administration Portal, click **Downloads**.

2 Under **Administration**, click **Download Firebox SSL VPN Gateway Administration Tool Installer**.

3 Select a location to save the installation application and click **Save**.
The installation tool is downloaded to your computer.

4 After downloading the file, navigate to the location where it was saved and then double-click the file.

5 To install the Administration Tool, follow the instructions in the wizard.

6 To start the Administration Tool, click **Start > Programs > WatchGuard> Firebox SSL VPN Gateway Adminstration Tool > Firebox SSL VPN Gateway Administration Tool**.

7 In **Username** and **Password,** type the Firebox SSL VPN Gateway administrator credentials. The default user name and password are **root** and **rootadmin**. You can change the administrative password as described in "To change the administrator password" on page 33.

Publishing Settings to Multiple Firebox SSL VPN Gateways

If you have multiple Firebox SSL VPN Gateway appliances in your network, you can configure the settings once and then publish them to all of the appliances on the network. The settings on the **VPN Gateway Cluster** tab apply to individual Firebox SSL VPN Gateways. The general networking, logging, administration, certificate generation and installation, and licensing are configured on the **VPN Gateway Cluster** tab. The settings on all other tabs in the Administration Tool can be published to multiple Firebox SSL VPN Gateways.

To publish Firebox SSL VPN Gateway settings

1 Click the **Publish** tab.

2 Click **Publish to all gateways**.

Each Firebox SSL VPN Gateway configured on the **VPN Gateway Cluster** tab is listed on the **Publish** tab. The following synchronization messages appear in the **Sync Status** field for each appliance:

In Sync
The Firebox SSL VPN Gateway configuration is successfully published.

Not in Sync
A change was made in the settings but is not published.

Sync Failed
Unable to synchronize the Firebox SSL VPN Gateway. Check the appliance and try the synchronization again.

Unknown Status
The status of the Firebox SSL VPN Gateway cannot be determined. Check the appliance and try the synchronization again.

Product Activation and Licensing

For new product installations, you will need to activate your Firebox SSL VPN Gateway by submitting the included license key codes to your Live Security account. You access your LiveSecurity account by browsing to the WatchGuard website at *http://www.watchguard.com*, then clicking LiveSecurity® Service on the left.

There are two types of included license key codes with your Firebox SSL VPN Gateway: **Tunnel and tunnel upgrade capacity**, and **LiveSecurity Renewal and Tunnel Renewal**.

Upgrading the tunnel and tunnel upgrade license

In your Live Security account, under the Activation Center, you activate your product with the tunnel and tunnel upgrade license key codes. Upon submittal and processing, you will receive license files or feature keys that you must apply to the Firebox SSL VPN Gateway. You apply these license files using the

Firebox SSL VPN Gateway Administration Tool. To apply these license files, see "Managing Licenses" on page 36.

For future tunnel capacity upgrades, you will follow these same steps to increase the capacity of your Firebox® SSL VPN Gateway.

Upgrading the LiveSecurity Renewal and Tunnel Renewal license

In your Live Security account, under Your Activated Products, you can activate and extend your Live Security support service by submitting the Live Security Renewal and Tunnel Renewal license keys. This allows you continued access to the Live Security service for the Firebox SSL VPN Gateway appliance. Chapter 1, "Getting Started with Firebox SSL VPN Gateway," for more information about the LiveSecurity Service.

Note

You must have a current Live Security account to upgrade your software or to add more tunnel capacity.

Managing Licenses

Firebox SSL VPN Gateway licensing limits the number of concurrent user sessions to the number of licenses purchased. If you purchase 100 licenses, you can have 100 concurrent sessions at any time. When a user ends a session, that license is released for the next user. A user who logs onto the Firebox SSL VPN Gateway from more than one computer occupies a license for each session.

If all licenses are occupied, no additional connections can be opened until a user ends a session or the administrator uses the Firebox SSL VPN Gateway Real-Time Monitor to close a connection, thereby releasing a license. For information about using the Real-Time Monitor to close connections, see "Managing Client Connections" on page 133.

Licenses for the Firebox SSL VPN Gateway are installed using the Administration Tool. License files are generated based on the host name, using either the external IP address or FQDN of the Firebox SSL VPN Gateway. When the license is uploaded to the primary Firebox SSL VPN Gateway, the host identifier of the license file is compared with the host names of each Firebox SSL VPN Gateway installed on the same network. If a match is found, the license file is accepted. When the license is installed, it can then be published to all of the appliances in the cluster.

To manage licenses on the Firebox SSL VPN Gateway

1 On the administrative computer where you run the Firebox SSL VPN Gateway Administration Tool, create a license directory.

2 Copy the license file (.lic) that you downloaded to the license directory.

Note

It is recommended that you retain a local copy of all license files that you receive. When you save a backup copy of the configuration file, all uploaded license files are included in the backup. If you need to reinstall the Firebox SSL VPN Gateway server software and do not have a backup of the configuration, you will need the original license files. Store the license files on the administrative computer where you run the Administration Tool.

Do not overwrite any .lic files in the license directory. If another file in that directory has the same name, rename the newly received file. The Firebox SSL VPN Gateway software calculates your licensed features based on all .lic files that are uploaded to the Firebox SSL VPN Gateway.

Do not edit a .lic file or the Firebox SSL VPN Gateway software ignores any features associated with that license file. The contents of the file are encrypted and must remain intact. Should you copy, rename, or insert a license file multiple times, the Firebox SSL VPN Gateway uses only the original file and ignores any duplicate files.

To install a license file

1 Click the **VPN Gateway Cluster** tab and then click the **Licensing** tab.

2 Next to **Upload a license file**, click **Browse** and locate the .lic file that you want to upload.

3 Select the .lic file and then click **Open** to upload the license file.

4 If more than one Firebox SSL VPN Gateway is installed on the same network, on the **Publish** tab, click **Publish to all gateways**.

To remove the licenses, next to **Clear all licensing**, click **Remove All**.

Information about Your Licenses

The **Licensing** tab displays information about the licenses that are installed on the Firebox SSL VPN Gateway. This information includes:

- Total number of licenses available
- Number of licenses currently in use

In addition, you can download license logs that provide you with detailed information about license use. When the logs are downloaded, they are in a compressed file called license_logs.zip.

To download license logs

1 On the **Firebox SSL VPN Gateway Cluster** tab, click the **Licensing** tab.

2 Under **Information about this Firebox SSL VPN Gateway**, next to **Download licensing logs**, click **Download All**.

3 Select the location to download the files and then click **Save**.

When you make changes to licensing on the Firebox SSL VPN Gateway, you can refresh the information that is displayed on the **Licensing** tab.

Testing Your License Installation

To test that licensing is configured correctly, create a test user and then log on using the Secure Access Client and credentials that you set up for the user.

To test your configuration

1 Open the Administration Tool.

2 Click the **Access Policy Manager** tab.

3 Right-click the Local Users folder in the left pane and click **New User**.

4 In the **New User** dialog box, in **User Name**, type a user name, and in **Password** and **Verify Password**, type the same password in each field, and click **OK**.

5 In a Web browser, type the address of the Firebox SSL VPN Gateway using either the IP address or fully qualified domain name (FQDN) to connect to either the internal or external interface. The format should be either *https://ipaddress* or *https://FQDN*.

6 Type the logon credentials. The **WatchGuard Firebox SSL VPN Gateway** portal page appears.

7 Click **My own computer** and then click **Connect**.
The Secure Access Client connection icon appears in the notification area, indicating a successful connection.

The initial configuration is complete. After completing the initial configuration, you can configure accessible networks so you can connect to all of your network resources, such as email, Web servers, and file shares as if you are in the office. To test your configuration, try connecting to the applications and resources that are available from the corporate network.

Blocking External Access to the Administration Portal

By default, if the Firebox SSL VPN Gateway is configured to use both network adapters, the external adapter can be used to access the Administration Portal from outside the firewall. To block access to the Administration Portal from the external adapter, clear the check box for this option.

To block external access to the Administration Portal

1 Click the **VPN Gateway Cluster** tab.

2 On the **Administration** tab, clear the check box for **Enable External Administration**.

3 Click **Apply Change**.

Using Portal Pages

The Firebox SSL VPN Gateway provides logon access using five portal pages. The portal page users see depends on the configuration of the Firebox SSL VPN Gateway. These include:

- Using the default portal page that provides full Secure Access Client and kiosk mode options. The default portal page is the only one that can be customized with your company name and logo.
- Redirecting the user to the Web Interface logon page.
- Providing a portal page that allows users the choice of logging on using Secure Access Client, the Web Interface, or kiosk mode.
- Pre-authentication Web page that appears when a pre-authentication policy is configured on the Firebox SSL VPN Gateway.
- Redirection to a Web page when double-source authentication is configured on the Firebox SSL VPN Gateway and the user logs on using Web access.

Using the Default Portal Page

Note

You can also include links to the Secure Access Client and kiosk mode on your Web site, as described in "Linking to Clients from Your Web Site" on page 41.

By default, users see a WatchGuard Firebox SSL VPN Gateway portal page when they open https://*Firebox SSL VPN Gateway_IP_or_hostname*. For samples of the default portal pages for Windows, Linux, and Java, see "Using the Access Portal" on page 118.

Several portal page templates that can be customized are provided. One of the templates includes links to both the Firebox SSL Secure Access Client and kiosk mode. Customization of the default portal page can be as simple as replacing the logo.

The text for **My own computer** and **A public computer** uses a variable to insert the text into the template. The text in these two sections cannot be changed.

The other two templates include links to just one of the clients. You choose a template based on the access that you want to provide on a group basis. For example, you might want to provide access to both clients to some users and access only to the Firebox SSL Secure Access Client or kiosk mode for other users. You can do that by adding custom portal pages to the Firebox SSL VPN Gateway and then specifying the portal page to be used for each user group.

Note

If you want to add text to the template or make format changes, you need to consult with someone who is familiar with HTML. Changes to the templates other than those described in this section are not supported.

The portal page templates are available from the Downloads page of the Administration Portal in the section **Sample Portal Page Templates**.

Downloading and Working with Portal Page Templates

The portal page templates include variables that the Firebox SSL VPN Gateway replaces with the current user name and with links that are appropriate for the connecting computer (Windows 2000 or higher, or Linux).

If you also have users on platforms such as Macintosh, Windows 95, or Windows 98, you can provide them access to the Java-based kiosk mode by inserting the appropriate variable in the template(s) used by those groups, as described in this section. The variables that can be used in templates are described in the following table.

Variable	Content inserted by variable
$citrix_username;	Name of logged on user.
$citrix_portal;	Links to both the Firebox SSL Secure Access Client and kiosk mode.
$citrix_portal_full_client_only;	Link to the Firebox SSL Secure Access Client only.
$citrix_portal_kiosk_client_only;	Link to kiosk mode only.
$citrix_activex_object_include	Inserts the ActiveX control that starts the client portal page.

A template can include only one of the three variables that start with $citrix_portal.

When choosing a template that is appropriate for a group, you need to know only whether the group should have access to both the Firebox SSL Secure Access Client and kiosk mode or just one of the clients. The Firebox SSL VPN Gateway detects the user's platform (Windows, Linux, Java) and inserts the appropriate links into the templates that you upload to the Firebox SSL VPN Gateway.

To download the portal page templates to your local computer

1 In the Firebox SSL VPN Gateway Administration Portal, click **Downloads**.

2 Under **Sample Portal Page Templates**, right-click one of the links, click **Save Target as,** and specify a location in the dialog box.

To work with the templates for Windows and Linux users

1 Determine how many custom portal pages that you need. You can use the same portal page for multiple groups.

Use this portal page:	To include links to these clients:
vpnAndKioskClients.html	Firebox SSL Secure Access Client and kiosk mode.
vpnClientOnly.html	Firebox SSL Secure Access Client only.
kioskClientOnly.html	Kiosk mode only.

2 Make a copy of each template that you will use and name the template, using the extension .html.

3 Open the file in Notepad or an HTML editing application.

4 To replace the WatchGuard image, locate the following line in the template:

5 Replace **citrix-logo.gif** with the filename of your image. For example, if your image file is named logo.gif, change the line to:

An image file must have a file type of GIF or JPG. Do not change other characters on that line.

6 Save the file.

Using the ActiveX Control

If you would like to use the ActiveX control to start the client portal page, insert the following code into the portal page template.

```
<html>
<head>
<title>Hello $citrix_username;</title>
$citrix_activex_object_include;
</head>
<body>
<img src="citrix-logo.gif">
<br/><br/>
<b>Hello $citrix_username;,</b>
<br/><br/>
$citrix_portal;
</body>
</html>
```

Installing Custom Portal Files on the Firebox SSL VPN Gateway

Custom portal pages and referenced image files must be installed on the Firebox SSL VPN Gateway.

To install a custom portal page or image on the Firebox SSL VPN Gateway

1 Click the **Portal Page Configuration** tab.

2 Click **Add File**.

3 In **File Identifier**, type a name that is descriptive of the types of users who use the portal page.
The file name can help you later when you need to associate the portal page with a group. For example, you might have a primary portal page used by many groups and a separate portal page used only by guests. In that case, you might identify the files as Primary Portal and Guest Portal. Alternatively, you might have several portal pages that correspond to user groups and use names such as Admin Portal, Student Portal, IT Portal.

4 In **File Type**, select the type.

5 Portal pages must be an HTML file. Any images referenced from an HTML page must be either GIF or JPG files.

6 Click **Upload File**.

7 Navigate to the file and click **Open**.
The file is loaded on the Firebox SSL VPN Gateway.

To remove a portal file from the Firebox SSL VPN Gateway

On the **Portal Page Configuration** tab, select the page identifier in the list and click **Remove Selected File**.

Enabling Portal Page Authentication

By default, a user must log on to the portal page and then again to the Firebox SSL Secure Access Client or kiosk mode. You can eliminate the portal page logon step using either of the following methods:

- You can set a global policy that disables authentication for the portal page and that specifies the portal page that displays for all users. This global policy overrides any portal page selections for groups.
- You can include links to the Firebox SSL Secure Access Client and kiosk mode directly on your Web site, as described in "Linking to Clients from Your Web Site" on page 41.

To enable portal page authentication

1 Click the **Global Cluster Policies** tab.

2 Under **Advanced Options**, select **Enable Portal Page Authentication**.

3 Click **Submit**.

Linking to Clients from Your Web Site

You can also provide your users links to the Firebox SSL Secure Access Client and kiosk mode from your Web site. The links launch the clients for Windows or direct the user to a page that explains how to download and install the client for Linux.

To include links to the Firebox SSL Secure Access Client and kiosk mode on your Web site

1 Add the following code to the HEAD tag of the Web page that is to contain the links:

```
<object id="Net6Launch" type="application/x-oleobject"
classid="CLSID:7E0FDFBB-87D4-43a1-9AD4-41F0EA8AFF7B"
codebase="net6helper.cab#version=2,1,0,6">
</object>
```

2 Add the links as follows to the Web page.

Client:	Link to:
Firebox SSL Secure Access Client (Windows/Java)	https://*ipAddress*/CitrixSAClient.exe
Kiosk mode (Windows/Java)	https://*ipAddress*/net6javakiosk_applet.html
Firebox SSL Secure Access Client (Linux)	https://*ipAddress*/full_linux_instructions.html where *ipAddress* is the address of the Firebox SSL VPN Gateway. This page includes a link to the Linux installer executable.

Multiple Log On Options using the Portal Page

Users can have the option to log on using Secure Access Client, the Web Interface, or kiosk mode from one Web page. This portal page cannot be configured like the default portal page. The user is presented with three icons and users can choose which method they want to use to log on to the Firebox SSL VPN Gateway. These are:

Secure Desktop Access

This icon starts the Secure Access Client.

Secure Application Access

This icon redirects the user to the Web Interface to log on.

Secure Kiosk Access

This icon logs on using kiosk mode.

This portal page is displayed only when the **Redirect to URL** and **Show "Launch Client" option page** check boxes are selected on the **Gateway Portal** tab.

To configure multiple log on options

1 On the **Access Policy Manager** tab, right-click a group in the left pane and then click **Properties**.

2 On the **Gateway Portal** tab, select **Redirect to URL**.

3 In **Portal homepage**, type the path of the server that is hosting the Web Interface.

4 In **Proxy Server,** type the IP address or FQDN of the server that is hosting the Web Interface.

5 To secure the connection, click **Use SSL/TLS**.

6 To provide Secure Access Client log on, select **Show "Launch Client" option page**.

Pre-Authentication Policy Portal Page

If a pre-authentication policy is configured on the Firebox SSL VPN Gateway, when the user connects using a Web address, a Web page appears while the policy is checked against the user's computer. If the client computer passes the pre-authentication policy check, users are then connected to the portal page where they can connect to the Firebox SSL VPN Gateway using their credentials. If the pre-authen-

tication policy check fails, the users receive an error message instructing them to contact their system administrator.

For more information about pre-authentication policies, see “Global policies” on page 96.

Double-source Authentication Portal Page

When the Firebox SSL VPN Gateway is configured to require users to log on using two types of authentication, such as LDAP and RSA SecurID, they are directed automatically to the Web page or Secure Access Client dialog box and users enter their user name and passwords.

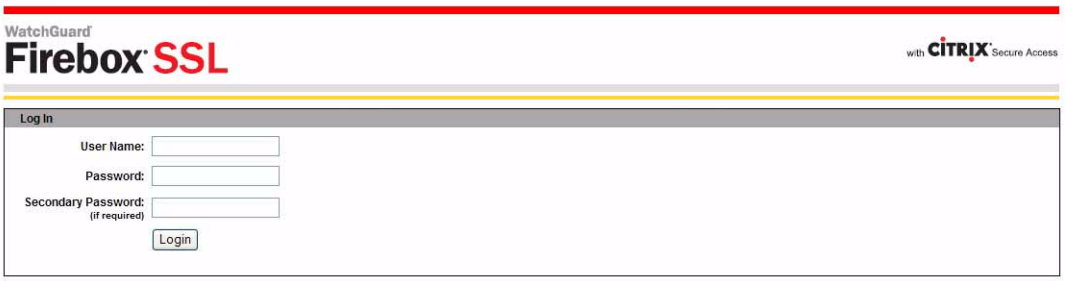
Note

When a user logs on using double authentication, the authentication is checked in the opposite order that is configured in the realm.For example, if the primary authentication type is LDAP and the secondary is RSA SecurID, the SecureID credentials are checked first, and then the LDAP credentials. If the user log on fails the first authentication, the second authentication is not checked.

For more information about double-source authentication, see “Configuring Double-Source Authentication” on page 85.

Connecting Using a Web Address

Users can connect to the Firebox SSL VPN Gateway using a Web browser by typing the Web address, such as https://vpn.mycompany.com. When the IP address or FQDN of the Firebox SSL VPN Gateway is entered and double-source authentication is configured, users are routed automatically to the logon portal page as shown below.



Double-source authentication portal page

After entering the user name, the user then enters the passwords for each authentication type. After the credentials are entered, the specified portal page appears and the user completes the connection from this portal page. The connection can be either full access or kiosk mode.

The double-source authentication portal page cannot be customized.

Connecting Using Secure Access Client

Users can connect to the Firebox SSL VPN Gateway using the Secure Access Client that is downloaded and installed on their computer. When double-source authentication is configured, users see a dialog box that requires their user name and passwords for each authentication type. After the users enter the credentials, they click **Connect**.

Saving and Restoring the Configuration

When you upgrade the Firebox SSL VPN Gateway, all of your configuration settings, including uploaded certificates, licenses, and portal pages, are restore automatically. However, if you reinstall the Firebox SSL VPN Gateway software, you must manually restore your configuration settings.

Note

Before using the Recovery CD to reinstall the Firebox SSL VPN Gateway software, save your configuration. Reinstalling the Firebox SSL VPN Gateway software returns the Firebox SSL VPN Gateway to its preconfigured state.

If you saved your configuration settings, as described in this section, you can easily restore them.

Note

You can also save and restore configuration settings from the **Maintenance** tab of the Administration Portal.

To save the Firebox SSL VPN Gateway configuration

1 In the Administration Tool, click the **VPN Gateway Cluster** tab.

2 Open the dialog box for the appliance.

3 On the **Administration** tab, by **Save the current configuration**, click **Save Configuration**.

4 Save the file, named **config.restore**, to your computer.
The entire Firebox SSL VPN Gateway configuration, including system files, uploaded licenses, and uploaded server certificates, is saved.

To restore a saved configuration

1 In the Administration Tool, click the **VPN Gateway Cluster** tab.

2 On the **Administration** tab, by **Upload a Server Upgrade or saved Config,** click **Browse**.

3 Locate the file named config.restore and click **Open**.
After the configuration file is uploaded, the Firebox SSL VPN Gateway restarts. All of your configuration settings, licenses, and certificates are restored.

4 If you use RSA SecurID authentication, you must reset the node secret on the RSA ACE/Server, as described in "Resetting the node secret" on page 82. Because the Firebox SSL VPN Gateway was reimaged, the node secret no longer resides on it and attempts to authenticate with the RSA ACE/Server fail.

Upgrading the Firebox SSL VPN Gateway Software

The software that resides on the Firebox SSL VPN Gateway can be upgraded when new releases are made available.

To upgrade the Firebox SSL VPN Gateway

1 In the Firebox SSL VPN Gateway Administration Tool, click the **VPN Gateway Cluster** tab, select the appliance, and then click the **Administration** tab.

2 In **Upload a Server Upgrade or Saved Config**, click Browse.

3 Locate the upgrade file that you want to upload and click **Open**.
The file is uploaded and the Firebox SSL VPN Gateway restarts automatically.
When you upgrade the Firebox SSL VPN Gateway, all of your configuration settings are saved. For information about saving and restoring a configuration, see "Saving and Restoring the Configuration" on page 44.

Restarting the Firebox SSL VPN Gateway

After making changes to the Firebox SSL VPN Gateway, you might need to restart the service.

To restart the Firebox SSL VPN Gateway

1 From the Administration Tool, click the **VPN Gateway Cluster** tab and select the appliance that needs to be restarted.

2 On the **Administration** tab, next to **Restart the server**, click **Restart**, or from the Administration Portal, go to the **Maintenance** tab and next to **Restart the Server**, click **Restart.**

Shutting Down the Firebox SSL VPN Gateway

Never shut down the Firebox SSL VPN Gateway by powering it off. Use the command in the Administration Tool to shut down the device. Use the power switch only to power on the device.

To shut down the Firebox SSL VPN Gateway

1 From the Administration Tool, click the **VPN Gateway Cluster** tab, and select the appliance that needs to be shut down.

2 On the **Administration** tab, next to **Shut down the server,** click **Shut down**.

3 Use the power switch to switch off the device.

Note

You can also shut down and restart the Firebox SSL VPN Gateway from the **Maintenance** page of Administration Portal.

Firebox SSL VPN Gateway System Date and Time

The system time displays on the right side of the taskbar in the Administration Desktop window. To view the system date, mouse over the system time.

To view a calendar, click the system time. Click the system time again to hide the calendar.

To change the system date and time

1 In the Administration Tool, click the **VPN Gateway Cluster** tab, select the appliance, and then click the **Date** tab.
2 In **Time Zone**, select a time zone.
3 In **Date**, type the date and time.
4 Click **Submit**.

Network Time Protocol

The Network Time Protocol transmits and receives time over TCP/IP networks. The Network Time Protocol is useful for synchronizing the internal clock of computers on the network to a common time source.

If you have a Network Time Protocol server in your secure network, you can use the Firebox SSL VPN Gateway Administration Tool to configure the Firebox SSL VPN Gateway to synchronize the time with the Network Time Protocol server.

To synchronize the Firebox SSL VPN Gateway with a Network Time Protocol server

1 In the Firebox SSL VPN Gateway Administration Tool, click the **VPN Gateway Cluster** tab.
2 Click the **Date** tab.
3 In **Synchronization Mode**, click **Network Time Protocol (NTP)**.
4 In **NTP Server**, type the FQDN of the server.
5 In **Synchronization Interval,** select a schedule to perform updates.

Allowing ICMP traffic

Internet Control Message Protocol (ICMP) traffic to the Firebox SSL VPN Gateway is disabled by default. To enable ICMP traffic, use the **VPN Gateway Cluster > Administration** tab.

When ICMP traffic is enabled, users can ping servers on the internal, secure network. The Firebox SSL VPN Gateway itself cannot receive ICMP traffic.

To enable ICMP traffic

1 In the Administration Tool, click the **VPN Gateway Cluster** tab and select the appliance.
2 On the **Administration** tab, select **Enable ping**.
3 Click **Apply Change**.

CHAPTER 4

Configuring Firebox SSL VPN Gateway Network Connections

The Firebox SSL VPN Gateway has two network adapters that can be configured to work on your network. The **VPN Gateway Cluster** > **General Networking** tabs in the Administration Tool are used to configure most network settings.

The following topics describe how to configure Firebox SSL VPN Gateway network connections:

- Configuring Network Information
- Configuring Firebox SSL VPN Gateway Failover
- Controlling Network Access
- Enabling Split Tunneling
- Denying Access to Groups without an ACL

Note

When you have a working configuration, it is recommended that you back up the configuration as described in "Saving and Restoring the Configuration" on page 44.

The configuration instructions throughout those topics assume the following setup:

- The Firebox SSL VPN Gateway is installed.
- The devices to which you are connecting the Firebox SSL VPN Gateway, such as a firewall or server load balancer, are already part of a working configuration. This guide does not cover the steps for configuring application or Web servers, firewalls, or a server farm with a server load balancer.

Configuring Network Information

You define the connections between the Firebox SSL VPN Gateway and your network on the **Network** tab.

The network adapter settings are configured on the **VPN Gateway Cluster** tab in the Firebox SSL VPN Gateway Administration Tool. On the **VPN Gateway Cluster** tab, you can configure the following:

- The **General Networking** tab is where the network adapters that are installed on the Firebox SSL VPN Gateway are configured
- The **Name Service Providers** tab is where the DNS and WINS servers are configured

- The **Routes** tab is where dynamic and static routes are configured
- The **Failover Servers** tab is where multiple Firebox SSL VPN Gateway's are configured

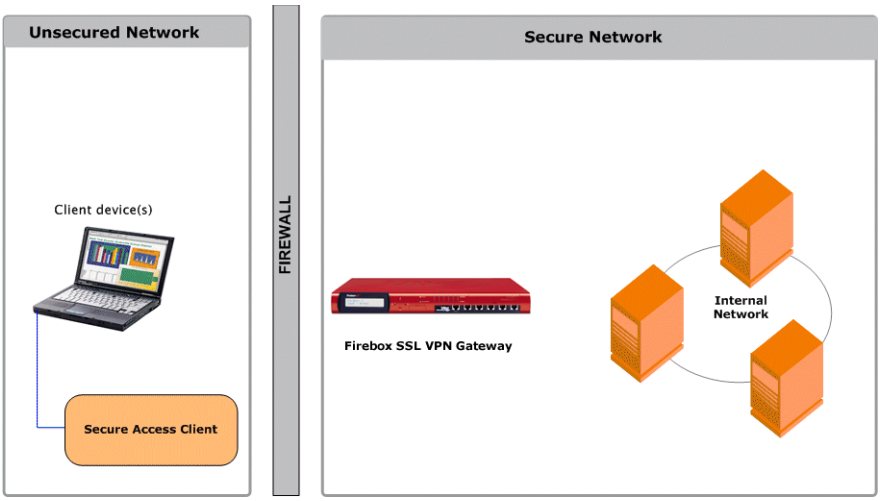
General Networking

The Firebox SSL VPN Gateway has two network adapters installed. If two network adapters are used, then one network adapter communicates with the Internet and computers that are not inside the corporate network. The other network adapter communicates with the internal network.

If one network adapter is used, it has to be routable for internal resources using Network Address Translation (NAT). The Firebox SSL VPN Gateway network adapter settings are as follows:

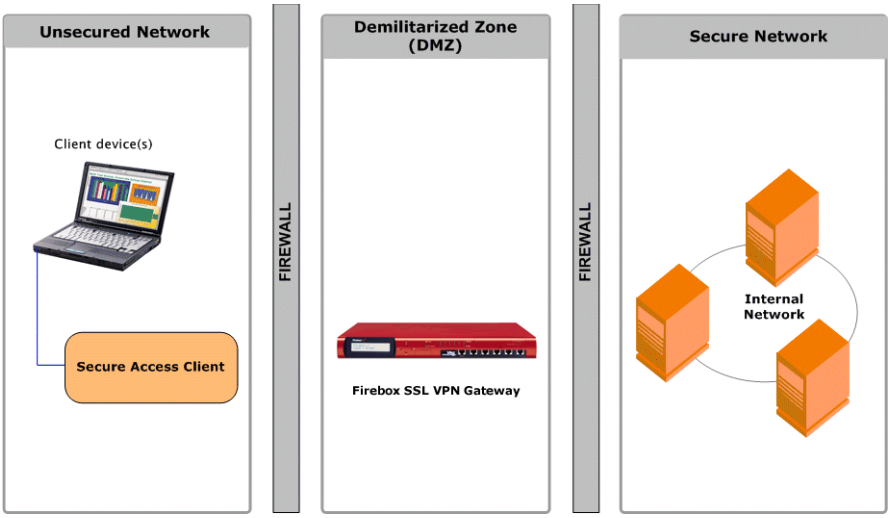
IP address *and* ***Subnet mask*** *for Interface 0 and, if used, Interface 1*

When connecting the Firebox SSL VPN Gateway to your network, you typically place it either inside of a firewall, inside of a server load balancer, or connected to two physical networks along side your firewall ("straddling" a firewall). If the Firebox SSL VPN Gateway is inside a firewall or connected to a server load balancer, choose **Use Only Interface 0**.



The Firebox SSL VPN Gateway located inside the firewall.

If the Firebox SSL VPN Gateway is in the DMZ, choose **Use both interfaces**. Use Interface 0 for the external connection and Interface 1 for the internal connection.



The Firebox SSL VPN Gateway in the DMZ.

For more information, see "Connecting to a Server Load Balancer" on page 28.

External Public FQDN

The Firebox SSL VPN Gateway uses the external IP address or FQDN to send its response to a request back to the correct network connection. If the external IP address is not specified, the Firebox SSL VPN Gateway sends responses out through the interface where the gateway is identified. If the external IP address is specified, the Firebox SSL VPN Gateway sends all connections to the interface with the specified host name or IP address.

Duplex mode

This is the direction of the transmission of data. Choices are either auto, full duplex, or half duplex. Use the default setting, auto, unless you need to change it.

MTU

The maximum transmission unit that defines the maximum size of each transmitted packet. The default is 1500. Use the default setting unless you need to change it.

VPN port

This is the incoming port on the Firebox SSL VPN Gateway that is used for VPN connections. The default is port 443.

The Default Gateway has the following two settings:

IP address

This is the IP address of the default gateway device, such as the main router, firewall, or server load balancer, depending on your network configuration. This should be the same as the Default Gateway setting that is on computers on the same subnet.

For information about the relationship between the Default Gateway and dynamic or static routing, see "Dynamic and Static Routing" on page 51.

Gateway Interface

This is the network adapter on the Firebox SSL VPN Gateway with which the Default Gateway communicates.

Note

IP pooling is configured per groups, as described in "Enabling IP Pooling" on page 94.

Name Service Providers

Name resolution is configured on the **Name Service Providers** tab. You can specify the following:

DNS Server 1, DNS Server 2, DNS Server 3

These are the IP address of the first, second, and third DNS servers.

DNS suffixes

These are the DNS suffixes of the servers. Each entry in the list is separated by a space. Each entry should follow the format of site.com. Do not precede a suffix with a dot ("."), such as .site.com.

By default, the Firebox SSL VPN Gateway checks a user's remote DNS only. If you want to allow failover to a user's local DNS, you need to enable split DNS.

WINS Server

This is the IP address of the WINS server.

To have client connections communicate with the WINS Server, the IP address must be manually added to the Accessible Networks list on the **Global Cluster Policies** tab. For more information, see "Controlling Network Access" on page 56. The IP address must also be added as a network resource on the **Access Policy Manager** tab and added to the user group(s). For more information, see "Defining network resources" on page 99.

To enable split DNS

1 On the **Access Policy Manager** tab, in the left pane, right-click a group and click **Properties**.

2 On the **Networking** tab, select **Enable split-DNS**.

The Firebox SSL VPN Gateway fails over to the local DNS only if the specified DNS servers cannot be contacted, but not if there is a negative response.

To edit the HOSTS file

You can add entries to the Firebox SSL VPN Gateway HOSTS file from the **Name Service Providers** tab. The Firebox SSL VPN Gateway uses the entries in the HOSTS file to resolve FQDNs to IP addresses.

When the Firebox SSL VPN Gateway attempts to translate an FQDN to an IP address, the Firebox SSL VPN Gateway checks its HOSTS file before connecting to DNS to perform the address translation. If the Firebox SSL VPN Gateway can translate the FQDN to an IP address using the information in the HOSTS file, it does not use DNS to perform the address translation.

You might want to add entries to the HOSTS file in an Firebox SSL VPN Gateway deployment where the network configuration prevents the Firebox SSL VPN Gateway from connecting to DNS to perform address translations. Also, adding entries to the HOSTS file can optimize performance because the Firebox SSL VPN Gateway does not have to connect to a different server to perform the address translations.

To add an entry to the HOSTS file

1 On the **Firebox SSL VPN Gateway Cluster** tab, open the window for an appliance.

2 Click the **Name Service Providers** tab.

3 Under **Edit the HOSTS file**, in **IP address**, enter the IP address that you want to associate with an FQDN.

4 In **FQDN**, enter the FQDN you want to associate with the IP address you entered in the previous step.

5 Click **Add**. The IP address and HOSTS name pair appears in the Host Table.

To remove an entry from the HOSTS file

1 Under **Host Table**, click the IP address and HOSTS name pair you want to delete.

2 Click **Remove**.

Dynamic and Static Routing

Configuring Network Routing

To provide access to internal network resources, the Firebox SSL VPN Gateway must be capable of routing data to the internal networks.

The networks to which the Firebox SSL VPN Gateway can route data are determined by the configuration of the Firebox SSL VPN Gateway routing table and the Default Gateway specified for the Firebox SSL VPN Gateway.

When the Firebox SSL VPN Gateway receives a packet, it checks its routing table. If the destination address of the packet is within a network for which a route exists in the routing table, the packet is routed to that network.

If the Firebox SSL VPN Gateway receives a packet, and its routing table does not contain a route for the destination address of the packet, the Firebox SSL VPN Gateway sends the packet to the Default Gateway. The routing capabilities of the Default Gateway then determine how the packet is routed.

The Firebox SSL VPN Gateway routing table must contain the routes necessary to route data to any internal network resource that a user may need to access.

You control how the Firebox SSL VPN Gateway routing tables are configured. You can select a Routing Information Protocol (RIP) option so that the routes are configured automatically by a RIP server, or you can select a static routing option and manually configure the routes.

You can configure the Firebox SSL VPN Gateway to listen for the routes published by your routing server(s) or to use static routes that you specify. The Firebox SSL VPN Gateway supports the Routing Information Protocol (RIP and RIP 2).

The **Default Gateway** field on the **General Networking** tab is relevant to both dynamic and static routing.

Enable Dynamic Gateway

If this option is enabled, the default gateway is based on the routing table, not on the value entered in the Default Gateway field on the General Networking tab.

Static Routing

If you add a static route, choose the Firebox SSL VPN Gateway network adapter that is not being used by the default gateway.

Configuring Dynamic Routing

When dynamic routing is selected, the Firebox SSL VPN Gateway operates as follows:

- It listens for route information published through RIP and automatically populates its routing table.
- If the Dynamic Gateway option is enabled, the Firebox SSL VPN Gateway uses the Default Gateway provided by dynamic routing, rather than the value specified on the **General Networking** tab.
- It disables any static routes created for the Firebox SSL VPN Gateway. If you later choose to disable dynamic routing, any previously created static routes appear again in the Firebox SSL VPN Gateway routing table.

To configure dynamic routing

1 Click the **VPN Gateway Cluster** tab and then click the **Routes** tab.

2 In **Select routing type**, select **Dynamic Routing (RIP)**.
Selecting this option disables the static routes area. If static routes are defined, they do not display in the routing table although they are still available if you want to switch back to static routing.

3 Click **Enable Dynamic Gateway** to use the default gateway provided by the routing server(s).
Selecting this check box disables use of the Default Gateway that is specified on the General Networking tab.

4 In **Routing Interface**, choose the Firebox SSL VPN Gateway network adapter(s) to be used for dynamic routing. Typically, your routing server(s) are inside your firewall, so you would choose the internal network adapter for this setting.

5 Click **Submit**.

Dynamic routes are not displayed in the Firebox SSL VPN Gateway routing table.

Enabling RIP Authentication for Dynamic Routing

To enhance security for dynamic routing, you can configure the Firebox SSL VPN Gateway to support RIP authentication.

Note

Your RIP server must transmit RIP 2 packets to use RIP authentication. RIP 1 does not support authentication.

To support RIP authentication, both the RIP server and the Firebox SSL VPN Gateway must be configured to use a specific authentication string. The RIP server can transmit this string as plain text or encrypt the string with MD5.

If the RIP server encrypts the authentication string with MD5, you must also select the MD5 option on the Firebox SSL VPN Gateway.

You can configure the Firebox SSL VPN Gateway to listen for the RIP authentication string on Interface 0, Interface 1, or both interfaces.

To enable RIP authentication for dynamic routing

1 On the **Firebox SSL VPN Gateway Cluster** tab, open the window for an appliance.

2 Click the **Routes** tab.

3 In **Routing Interface**, select either **Interface 0**, **Interface 1**, or **Both** to specify the interface(s) on which the Firebox SSL VPN Gateway listens for the RIP authentication string.

4 Select the **RIP Authentication String for Interface** check box.

5 In the text box, type a text string that is an exact, case-sensitive match to the authentication string transmitted by the RIP server.

6 Select the **Enable RIP MD5 Authentication for Interface** check box if the RIP server transmits the authentication string encrypted with MD5.
Do not select this option if the RIP server transmits the authentication string using plain text.

7 Click **Submit**.

Changing from Dynamic Routing to Static Routing

Before you change from dynamic routing to static routing, you may want to save your dynamic routes to the static route table. Selecting this option saves the current RIP dynamic routing information as static routes.

If you change from dynamic routing to static routing, and you previously created static routes, the static routes reappear in the Firebox SSL VPN Gateway routing table.

If these static routes are no longer valid, or if no static routes were created previously, you might lose remote access to the Administration Tool and users could lose access to the internal network resources until you manually configure the static routes.

Saving the current RIP dynamic routing information as static routes when you switch from dynamic routing to static routing allows you to maintain connectivity until you properly configure the static routes.

To save dynamic routes to the static route table

1 On the **Firebox SSL VPN Gateway Cluster** tab, open the window for the appliance.

2 Click the **Routes** tab.

3 Click **Save to static routes**.

After you save the dynamic route, you can switch to static routing.

Configuring a Static Route

When setting up communication with another host or network, a static route might need to be added from the Firebox SSL VPN Gateway to the new destination if you do not use dynamic routing.

Set up static routes on the Firebox SSL VPN Gateway adapter not being used by the Default Gateway that is specified on the **General Networking** tab.

For an example static route setup, see "Static Route Example" on page 54.

To add a static route

1 Click the **VPN Gateway Cluster** tab and then click the **Routes** tab.

2 In **Select routing type**, select **Static Routing**.

3 Under **Add Static Route**, in **Destination LAN IP Address**, type the IP address of the destination local area network.

4 In **Subnet Mask**, type the subnet mask for the gateway device.

5 In **Gateway**, type the IP address for the default gateway. If you do not specify a gateway, the Firebox SSL VPN Gateway can access content only on the local network.

6 In **Interface**, select the network adapter for the static route. The default is eth0.

7 Click **Add Static Route**.

8 On the **General Networking** tab, click **Submit**.
The route name appears in the Static Routes list.

To test a static route

1 From the Firebox SSL VPN Gateway serial console, type **1** (ping).

2 Enter the host IP address for the device you want to ping and press **Enter**.

If you are successfully communicating with the other device, messages appear saying that the same number of packets were transmitted and received, and zero packets were lost.

If you are not communicating with the other device, the status messages indicate that zero packets were received and all the packets were lost. Return to Step 1 and recreate the static route.

To remove a static route

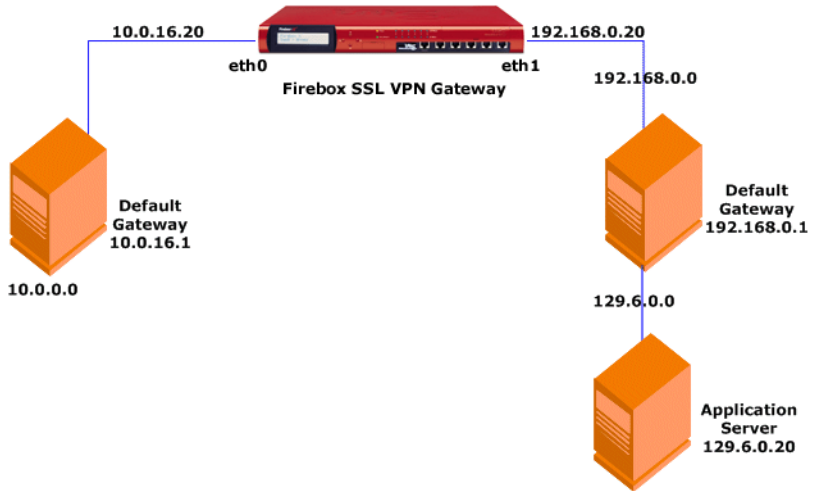
1 Click the **VPN Gateway Cluster** tab and then click the **Routes** tab.

2 In the Static Route table, select each route that you want to delete.

3 Click **Remove Route.**

Static Route Example

Suppose the IP address of the eth0 port on your Firebox SSL VPN Gateway is 10.0.16.20 and there is a request to access information at 129.6.0.20 to which you currently do not have a path. You can create a static route through the network adapter that is not set as your Firebox SSL VPN Gateway default gateway, and out to the requested network address, as shown in the following figure:



Network topology showing a static route.

This shows these connections:

- The eth0 adapter (10.0.16.20) leads to the default gateway (10.0.16.1), which connects to the rest of the 10.0.0.0 network.
- The eth1 adapter (192.168.0.20) is set to communicate with the 192.168.0.0 network and its gateway (192.168.0.1). Through this gateway, the eth1 port can communicate with the 129.6.0.0 network and the server at IP address 129.6.0.20.

To set up the static route, you need to establish the path between the eth1 adapter and IP address 129.6.0.20.

To set up the example static route

1 Click the **VPN Gateway Cluster** tab and then click the **Routes** tab.
2 In **Destination LAN IP Address**, set the IP address of the destination LAN to **129.6.0.0**.
3 In **Subnet Mask**, set the subnet mask for the gateway device.
4 In **Gateway**, set the IP address of the default gateway to **192.168.0.1**.
5 In **Interface**, select **eth1** as the gateway device adapter.
6 Click **Add Static Route**.

Configuring Firebox SSL VPN Gateway Failover

The Firebox SSL VPN Gateway can be configured to fail over to multiple Firebox SSL VPN Gateway appliances. Because Firebox SSL VPN Gateway failover is active/active, you can use each Firebox SSL VPN Gateway as a primary gateway for a different set of users.

During the initial connection from the Secure Access Client, the Firebox SSL VPN Gateway provides the failover list to the client. If the client loses the connection to the primary Firebox SSL VPN Gateway, it iterates through the list of failover appliances. If the primary Firebox SSL VPN Gateway fails, the connection waits for 20 seconds and then goes to the failover list to make the connection. The client performs a DNS lookup for the first failover appliance and tries to connect. If the first failover Firebox SSL VPN Gateway is not available, the client tries the next failover appliance. When the client successfully connects to a failover Firebox SSL VPN Gateway, the client is prompted to log on.

To specify Firebox SSL VPN Gateway failover

1 Click the **VPN Gateway Cluster** tab and then click the **Failover Servers** tab.
2 In **Failover Server 1**, **Failover Server 2**, and/or **Failover Server 3**, type the external IP address or the fully qualified domain name (FQDN) of the Firebox SSL VPN Gateway(s) to be used for failover operation.
The Firebox SSL VPN Gateways are used for failover in the order listed.
3 In **Port**, type the port number. The default is 443.
4 Click **Submit**.

Configuring Internal Failover

Configuring the client's local DNS settings enables the Secure Access Client to connect to the Firebox SSL VPN Gateway from inside the firewall. When internal failover is configured, the client will failover to the internal IP address of the Firebox SSL VPN Gateway if the external IP address cannot be reached.

To enable internal failover

1 Click the **Global Cluster Policies** tab.
2 Under **Advanced Options**, select **Enable Internal Failover**.

When this check box is selected, the internal IP address of the Firebox SSL VPN Gateway is added to the failover list. If you disabled external administrator access, port 9001 is unavailable. If you want to con-

nect to port 9001 when you are logged on from an external connection, configure IP pools and connect to the lowest IP address in the IP pool.

Controlling Network Access

Configuring Network Access

After you configure the appliance to operate in your network environment, the next step is to configure network access for the appliance and for groups and users.

The steps to configure network access are:

- **Step 1: Configuring networks to which clients can connect.** By default, clients cannot connect to any networks. The first step in configuring network access is to specify the networks that clients can connect to, using the **Global Cluster Policies** tab.
- **Step 2: Configuring authentication and authorization.** Authentication defines how users log on and is configured using realms. Authentication types include local, NTLM, LDAP, RADIUS, RSA SecurID, and SafeWord. Authorization types include local, LDAP, RADIUS, NTLM, or no authorization. For more information about configuring authentication and authorization, see"Configuring Authentication and Authorization" on page 61.
- **Step 3: Configuring user groups.** User groups are used in conjunction with authorization. For example, if your users are connecting using LDAP, create an LDAP authentication realm, and then create a group. The names of the user group must be the same as that on the LDAP server. In addition, you can create local users on the Firebox SSL VPN Gateway for local authentication. Local users are then added to user groups. For information about configuring local users, see "Adding and Configuring Local Users and User Groups" on page 87.
- **Step 4: Configuring network access for groups.** After you configure your user groups, you then configure network access for the groups. This includes the network resources users in the group are allowed to access, application policies, kiosk connections, and end point policies.

For more information about configuring accessible networks, user groups, and network access for users, see"Adding and Configuring Local Users and User Groups" on page 87.

By default, the Firebox SSL VPN Gateway is blocked from accessing any networks. You must specify the networks that the Firebox SSL VPN Gateway can access, referred to as *accessible networks*. You then control user access to those networks as follows:

- You create network resource groups.
  A network resource group includes one or more network locations. For example, a resource group might provide access to a single application, a subset of applications, a range of IP addresses, or an entire intranet. What you include in a network resource group depends largely on the varying access requirements of your users. You might want to provide some user groups with access to many resources and other user groups with access to smaller subsets of resources. By allowing and denying a user group access to network resource groups, you create an access control list (ACL) for that user group.
- You specify whether or not any user group without an ACL has full access to all of the accessible networks defined for the Firebox SSL VPN Gateway.
  By default, user groups without an ACL have access to all of the accessible networks defined for the Firebox SSL VPN Gateway. This default operation provides simple configuration if most of your user groups are to have full network access. By retaining this default operation, you need to configure an ACL only for the user groups that should have more restricted access. The default operation can also be useful for initial testing.

You can change the default operation so that user groups are denied network access unless they are allowed access to one or more network resource groups.

- You configure ACLs for user groups by specifying which network resources are allowed or denied per user group.
  By default, all network resource groups are allowed and network access is controlled by the **Deny Access without ACL** option on the **Global Cluster Policies** tab. When you allow or deny one resource group, all other resource groups are denied automatically and the network access for the user group is controlled only through its ACL.
  If a resource group includes a resource that you do not want a user group to access, you can create a separate resource group for just that resource and deny the user group access to it.

The options just discussed are summarized in the following table.

ACL set for user group?	Deny access without ACL?	User group can access:
No	No	All accessible networks
Yes	No	Allowed resource groups
No	Yes	Nothing
Yes	Yes	Allowed resource groups

Specifying Accessible Networks

You must specify which networks the Firebox SSL VPN Gateway can access.

When configuring network access, the most restrictive policy must be configured first and the least restrictive last; for example, you want to allow access to everything on the 10.0.x.x network, but need to deny access to the 10.0.20.x network. Configure network access to 10.0.20.x first and then configure access to the 10.0.x.x network.

To give the Firebox SSL VPN Gateway access to a network

1 Click the **Global Cluster Policies** tab.

2 Under **Access Options**, in **Accessible Networks**, type a list of networks. Use a space or carriage return to separate the list of networks.

3 Click **Submit**.

Enabling Split Tunneling

You can enable *split tunneling* on the **Global Cluster Policies** tab to prevent the Secure Access Client from sending unnecessary network traffic to the Firebox SSL VPN Gateway.

When split tunneling is not enabled, the Secure Access Client captures all network traffic originating from a client computer, and sends the traffic through the VPN tunnel to the Firebox SSL VPN Gateway.

If you enable split tunneling, the Secure Access Client sends only traffic destined for networks protected by the Firebox SSL VPN Gateway through the VPN tunnel. The Secure Access Client does not send network traffic destined for unprotected networks to the Firebox SSL VPN Gateway.

When you enable split tunneling, you must enter a list of accessible networks on the **Global Cluster Policies** tab. The list of accessible networks must include all internal networks and subnetworks that the user may need to access with the Secure Access Client.

The Secure Access Client uses the list of accessible networks as a filter to determine whether or not packets transmitted from the client computer should be sent to the Firebox SSL VPN Gateway.

When the Secure Access Client starts, it obtains the list of accessible networks from the Firebox SSL VPN Gateway. The Secure Access Client examines all packets transmitted on the network from the client computer and compares the addresses within the packets to the list of accessible networks. If the destination address in the packet is within one of the accessible networks, the Secure Access Client sends the packet through the VPN tunnel to the Firebox SSL VPN Gateway. If the destination address is not in an accessible network, the packet is not encrypted and the client routes the packet appropriately.

To enable split tunneling

1 Click the **Global Cluster Policies** tab.

2 Under **Access Options**, click **Enable Split Tunneling**.

3 In **Accessible Networks**, type the IP addresses. Use a space or carriage return to separate the list of networks.

4 Click **Submit**.

Configuring User Groups

User groups define the resources the user has access to when connecting to the corporate network through the Firebox SSL VPN Gateway. Groups are associated with the local users list. After adding local users to a group, you can then define the resources they have access to on the **Access Policy Manager** tab. For more information about configuring local users, see "Configuring Properties for a User Group" on page 90.

When you enable authorization on the Firebox SSL VPN Gateway, user group information is obtained from the authentication server after a user is authenticated. If the group name that is obtained from the authentication server matches a group name created locally on the Firebox SSL VPN Gateway, the properties of the local group are used for the matching group obtained from the authentication servers.

Note

Important: Group names on authentication servers and on the Firebox SSL VPN Gateway must be identical and they are case-sensitive

Denying Access to Groups without an ACL

Each user should belong to at least one group that is defined locally on the Firebox SSL VPN Gateway. If a user does not belong to a group, the overall access of the user is determined by using access control lists (ACLs) that are defined by the **Deny access without access control list (ACL)** setting as follows:

If the Deny Access option is enabled, the user cannot establish a connection

If the Deny Access option is disabled, the user has full network access

In either case, the user can use kiosk mode, but network access within that session is determined by the **Deny access without access control list (ACL)** setting.

To deny access to user groups without an ACL

1 Click the **Global Cluster Policies** tab.

2 Under **Access Options**, select **Deny Access without ACL**.

3 Click **Submit**.

Improving Voice over IP Connections

Real-time applications, such as voice and video, are implemented over UDP. TCP is not appropriate for real-time traffic due to the delay introduced by acknowledgements and retransmission of lost packets. It is more important to deliver packets in real time than to ensure that all packets are delivered. However, with any tunneling technology over TCP, such real-time performances cannot be met.

The Firebox SSL VPN Gateway overcomes this issue by routing UDP packets over the secure tunnel as special IP packets that do not require TCP acknowledgements. Even if the packets get lost in the network, no attempt is made by either the client or the server applications to regenerate them, so real-time (UDP like) performance is achieved over a secure TCP-based tunnel.

When the Firebox SSL VPN Gateway is installed as a stand alone appliance, and users connect using the Secure Access Client, two-way communication is supported with the following voice over IP (VoIP) softphones:

- Avaya IP Softphone
- Nortel IP Softphone
- Cisco IP Softphone
- Cisco IP Communicator

Secure tunneling is supported between the manufacturer's IP PBX and the softphone software running on the client computer. To enable the VoIP traffic to traverse the secure tunnel, you must install the Secure Access Client and one of the softphones listed above on the same system. When the VoIP traffic is tunneled over the secure tunnel, the following softphone features are supported:

- Outgoing calls that are placed from the IP softphone
- Incoming calls that are placed to the IP softphone
- Bidirectional voice traffic

Enabling Improving Voice over IP Connections

Voice over IP (VoIP) traffic is carried over the UDP protocol. This kind of traffic is very sensitive to latency. The Firebox SSL VPN Gateway tunnels the UDP traffic through SSL connections. If you experience latency in your VoIP application, you can select the **Improving Voice over IP Connections** setting to minimize latency and improve the audio quality.

When you select this setting, the Firebox SSL VPN Gateway employs weaker encryption ciphers (56-bit). These weaker ciphers are used for all traffic that is transmitted using the UDP protocol, not just the VoIP traffic. Before selecting this option, you might want to consider the security implications of using these weaker ciphers to encrypt the UDP traffic.

The specific ciphers used to encrypt the UDP traffic include

- RSA EXP 1024, RC4 56 Bit, MD5
- RSA EXP 1024, RC4 56 Bit, SHA

Note

If the **Improving Voice over IP Connections** setting is not selected, the UDP traffic is encrypted using the symmetric encryption cipher that is specified in the **Select encryption type for client connections** setting on the **Global Cluster Policies** tab.

The encryption ciphers are negotiated between the client computer and the Firebox SSL VPN Gateway in the order listed. The first accepted method is the one chosen for the session.

To improve latency for UDP traffic

1 Click the **Global Cluster Policies** tab.

2 Under **SSL Options**, select **Improve latency for Voice over IP traffic**.

3 Click **Submit**.

CHAPTER 5

Configuring Authentication and Authorization

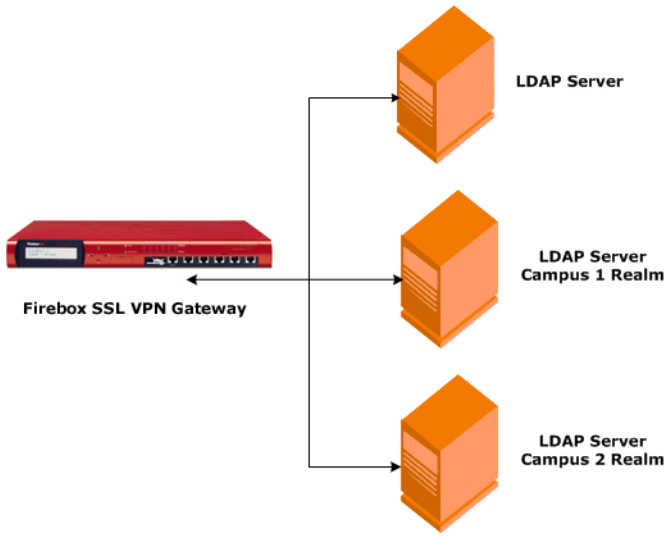
The Firebox SSL VPN Gateway supports several authentication types including LDAP, RADIUS, RSA SecurID, NTLM, and Secure Computing's SafeWord products.

The following topics describe how to configure Firebox SSL VPN Gateway authentication:

- Choosing When to Configure Authentication on the Firebox SSL VPN Gateway
- Configuring Authentication on the Firebox SSL VPN Gateway
- Configuring Local Authentication
- Configuring Local Users
- Configuring LDAP Authentication and Authorization
- Configuring RADIUS Authentication and Authorization
- Configuring RSA SecurID Authentication
- Configuring Secure Computing SafeWord Authentication
- Configuring NTLM Authentication and Authorization
- Configuring Double-Source Authentication

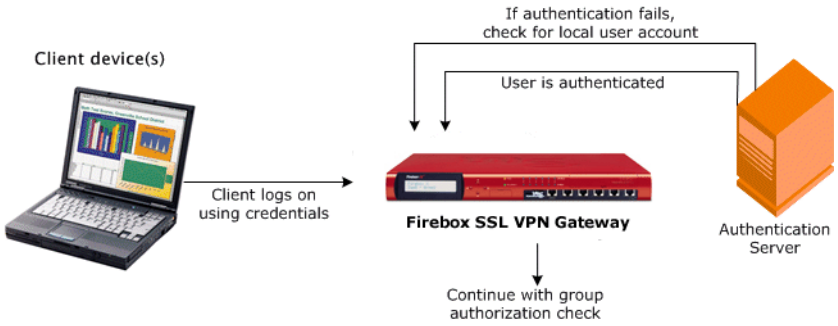
Configuring Authentication and Authorization

By default the Firebox SSL VPN Gateway authenticates users against a user list stored locally on the Firebox SSL VPN Gateway. You can configure the Firebox SSL VPN Gateway to use LDAP, RADIUS, RSA SecurID, SafeWord, or NTLM (Windows NT 4.0) authentication servers. The Firebox SSL VPN Gateway supports realm-based authentication to accommodate sites with more than one LDAP or RADIUS server or with a combination of SafeWord, LDAP, RADIUS, NTLM, and/or RSA SecurID authentication servers.



Communications between the Firebox SSL VPN Gateway and authentication servers.

If a user is not located on an authentication server or fails authentication on that server, the Firebox SSL VPN Gateway checks the user against the local user list, if the check box **Use the local user database on the Firebox SSL VPN Gateway** is selected on the **Authentication > Settings** tab.



Communication between the client, the Firebox SSL VPN Gateway, and the local user account.

After a user is authenticated, the Firebox SSL VPN Gateway performs a group authorization check by obtaining the user's group information from either an LDAP server, a RADIUS server, a Windows NT 4.0 server (for NTLM authorization), or the local group file (if not available on the LDAP or RADIUS server). If group information is available for the user, the Firebox SSL VPN Gateway then checks the network resources allowed for the group. LDAP authorization works with all supported authentication methods.

You can configure the Firebox SSL VPN Gateway to obtain an authenticated user's group(s) from an LDAP server. If the user is not located on the LDAP server, the Firebox SSL VPN Gateway checks its local group file if the check box **Use the local user database on the Firebox SSL VPN Gateway** is selected on the **Authentication > Settings** tab.

The group names obtained from the LDAP server are compared with the group names created locally on the Firebox SSL VPN Gateway. If the two group names match, the properties of the local group apply to the group obtained from the LDAP server.

Configuring Authentication without Authorization

The Firebox SSL VPN Gateway can be configured to authenticate users without requiring authorization. When users are not authorized, the Firebox SSL VPN Gateway does not perform a group authorization check. The settings from the Default user group are assigned to the user.

To remove authorization requirements from the Firebox SSL VPN Gateway

1 On the **Authentication** tab, select an authorization realm.
2 On the **Authorization** tab, in **Authorization type**, select **No authorization**.

The Default Realm

The Firebox SSL VPN Gateway has a permanent realm named Default with the following characteristics:

- For a new installation, the Default realm is configured for local authentication.
- The authentication type of the Default realm can be changed.
- The Default realm cannot be removed unless you immediately replace it with a new Default realm.
- The Default realm is assumed when a user enters only a user name when logging on to the Firebox SSL VPN Gateway.

When a user logs on to any other realm, the user must log on using *realmName\userName*. Therefore, if all of your users are authenticated against one authentication server, configure the Default realm for that type of authentication so that users do not have to enter a realm name when logging on.

Using a Local User List for Authentication

For a new installation, the Default realm is set to local authentication. This enables users to log on to the Firebox SSL VPN Gateway without having to enter a realm name.

If some users authenticate only against the local user list on the Firebox SSL VPN Gateway, you can keep the Default realm set to local authentication. Alternatively, you can create a different realm for local authentication and use the Default realm for another authentication type, as described in "To remove and create a Default realm".

If all users authenticate against authentication servers, you do not need a realm for local authentication. The Firebox SSL VPN Gateway can check the local user database on the appliance for authentication information if a user fails to authenticate on another authentication server. For example, If you are using LDAP and the authentication fails, users can log on using the local user database.

To authenticate using the local user list on the Firebox SSL VPN Gateway

1 On the **Authentication** tab, open the authentication realm on which you
2 want to configure local authentication.
3 Click the **Settings** tab.
4 Select **Use the local user database on the** Firebox SSL VPN **Gateway**.
5 Click **Submit**.

Note

This check box is unavailable if the realm is configured for local authentication

Configuring Local Users

You can create user accounts locally on the Firebox SSL VPN Gateway to supplement the users on authentication servers. For example, you might want to create local user accounts for temporary users, such as consultants or visitors, without creating an entry for those users on the authentication server. In that case, you add the user to the Firebox SSL VPN Gateway local user list as described in this section.

To add a user to another group, under **Local Users**, click and drag the user to the appropriate user group.

If a user is not a member of a group or groups you defined on the Firebox SSL VPN Gateway, the user receives the settings for the Default user group. If a user is part of a group other than the Default group, the user inherits only the settings of the Default group if the group is configured to receive those settings. For more information, see "Default group properties" on page 90.

To create a user on the Firebox SSL VPN Gateway

1 Click the **Access Policy Manager** tab.

2 In the left-pane, right-click **Local Users** and then click **New User**.

3 In **User Name**, type a user name. User names can contain spaces.

Note

Note: User names are not case-sensitive. Do not use a forward slash (/) in the user name or password. Passwords cannot begin or end with a space.

4 In **Password** and **Verify Password**, type the password for the user.
A user enters this password when logging on. A password must be six or more characters up to a maximum of 127 characters.

5 Click **OK**.

To delete a user from the Firebox SSL VPN Gateway

1 Click the **Access Policy Manager** tab.

2 In the left pane, right-click the user in the **Local Users** list and click **Remove**.

Adding Users to Multiple Groups

After creating the local user list, you can then add the users to groups that you created on the Firebox SSL VPN Gateway.

If you associate more than one group with a user account, the properties of the first group that you select on the **Group Priority** tab is used for the user.

To add a user to a group

Click the user in the **Local Users** list and drag it to a group.

Changing Password for Users

You can change the password for a user in the Administration tool.

To change a user's password

1 On the **Access Policy Manager** tab, right-click a user, and click **Set Password.**

2 Type the password twice and then click **OK**.

Using LDAP Authorization with Local Authentication

By default, the Firebox SSL VPN Gateway obtains an authenticated user's group(s) from the local group file stored on the Firebox SSL VPN Gateway. Alternatively, you can configure the Firebox SSL VPN Gateway to obtain an authenticated user's group(s) from an LDAP server. If the user is not located on the LDAP server, the Firebox SSL VPN Gateway checks its local group file.

To use LDAP authorization with local authentication

1 In the Firebox SSL VPN Gateway Administration Tool, click the **Authentication** tab.

2 Open the window for the realm that is configured for local authentication. This is the Default realm unless the authentication type was changed.

3 Click the **Authorization** tab.

4 In **Authorization Type**, select **LDAP Authorization**.

5 Complete the information for the LDAP server.
For a description of LDAP server settings, see "Using LDAP Servers for Authentication and Authorization" on page 73. For information about looking up LDAP server settings, see "Determining Attributes in your LDAP Directory" on page 78.

Changing the Authentication Type of the Default Realm

When a user logs on to the Default realm, the user does not have to specify a realm name. For any other realm, the user must specify a realm name when logging on. Thus, if most users are logging on to a non-local authentication realm, change the authentication type of the Default realm.

To change the authentication type of the Default realm, remove the Default realm and then immediately create a new one.

Configuring the Default Realm

The Firebox SSL VPN Gateway has a permanent realm named Default. The Default realm is preconfigured for local authentication. If you want to change the authentication method of the Default realm, it must be immediately replaced with a new Default realm.

The Default realm is assumed when a user enters only a user name when logging on to the Access Gateway. For any other realm, the user must specify a realm name when logging on. Thus, if most users are logging on to a non-local authentication realm, change the authentication type of the Default realm.

To change the authentication type of the Default realm, remove the Default realm

and then immediately create a new realm with the appropriate authentication

configuration.

To remove and create a Default realm

1 Click the **Authentication** tab.

2 Open the window for the Default realm.

3 On the **Action** menu, select **Remove Default realm**.
A warning message appears. Click **Yes**.
4 Under **Add an Authentication Realm**, in **Realm name**, type Default.

Note

Important: When creating a new Default realm, the word Default is case-sensitive and an uppercase D must be used.

5 Do one of the following:
- If configuring one authentication type, select **One Source** and click **Add**.
- If configuring double-source authentication, select **Two Source** and click **Add**.

6 In **Authentication type**, select the type of authentication and then click **OK**.
7 Configure the authentication settings. For more information, see:
- "Using a Local User List for Authentication" on page 63
- "Using LDAP Servers for Authentication and Authorization" on page 73
- "Using RADIUS Servers for Authentication and Authorization" on page 69
- "Using RSA SecurID for Authentication" on page 79
- "Using SafeWord for Authentication" on page 67
- "Configuring NTLM Authentication and Authorization" on page 83

Creating Additional Realms

You can create realms in addition to the Default realm. For example, you want the Default realm to be used for authentication to an LDAP server. If you want to use additional authentication methods for users, such as RADIUS, SafeWord, RSA SecurID, NTLM, or locally on the appliance, you can create realms for each of these. When the user logs on to realms that are not the Default realm, they need to type the realm name and their user name, such as *realm name**user name*.

Note

Note: Watchguard recommends that realm names map to their corresponding domain names. This enables users to log on using either *realm name**user name* or *user name@realm name*.

To create a realm

1 On the **Authentication** tab, under **Add an Authentication Realm**, in **Realm name**, type the name of the realm.
2 Do one of the following:
If users have one authentication type, click **One Source**.
-or-
If users have two authentication types, click **Two Source**.
3 Click **Add**.
4 In **Authentication type**, select the authentication method, and click **OK**.
If you are configuring double-source authentication, in **Primary authentication type**, select the type that users will log on to first. In **Secondary authentication type**, select the type that users will log on to second. For more information, see "Configuring Double-Source Authentication" on page 85.
5 Configure the settings for the realm and then click **Submit**.

Removing Realms

If you are retiring an authentication server or removing a domain server, you can remove any realm except for the realm named Default. You can remove the Default realm only if you immediately create a new realm named Default. For more information, see "Configuring the Default Realm" on page 65.

To remove a realm

1 On the **Authentication** tab, open the realm you want to remove.

2 On the **Action** menu, click **Remove *realm name* realm**.
The realm is removed.

Note

If you remove the Default realm and do not immediately replace it as described above, the Firebox SSL VPN Gateway retains the Default realm that you attempted to remove.

Using SafeWord for Authentication

Configuring Secure Computing SafeWord Authentication

The SafeWord product line provides secure authentication using a token-based passcode. After the passcode is used, it is immediately invalidated by SafeWord and cannot be used again.

The Firebox SSL VPN Gateway supports SafeWord authentication to the following Secure Computing products:

- SafeWord PremierAccess
- SafeWord for Citrix
- SafeWord RemoteAccess

Configuring the Firebox SSL VPN Gateway to authenticate using Secure Computing's SafeWord products can be done in several ways:

- Configure authentication to use a PremierAccess RADIUS server that is installed as part of SafeWord PremierAccess and allow it to handle authentication.
- Configure authentication to use the SafeWord IAS agent, which is a component of SafeWord RemoteAccess, SafeWord for WatchGuard, and SafeWord PremierAccess 4.0.
- Install the SafeWord Web Interface Agent to work with the WatchGuard Web Interface. Authentication does not have to be configured on the Firebox SSL VPN Gateway and can be handled by the WatchGuard Web Interface. This configuration does not use the PremierAccess RADIUS server or the SafeWord IAS Agent.

Configuring SafeWord Settings on the Access Gateway

When configuring the SafeWord server, you need the following information:

- The IP address of the Firebox SSL VPN Gateway. This should be the same as what is configured on the RADIUS server client configuration.
- A shared secret. This secret is also configured on the **Authentication** tab on the Firebox SSL VPN Gateway.
- The IP address and port of the SafeWord server.

Configure a SafeWord realm to authenticate users. The Firebox SSL VPN Gateway acts as a SafeWord agent authenticating on behalf of users logged on using Secure Access Client. If a user is not located on the SafeWord server or fails authentication, the Access Gateway checks the user against the local user list if **Use the local user database on the Access Gateway** is selected on the **Settings** tab.

To use SafeWord as the Default realm, remove the current Default realm and create a new one as described in "To remove and create a Default realm"

To configure SafeWord on the Access Gateway

1 In the Administration Tool, click the **Authentication** tab.

2 Under **Add an Authentication Realm**, in **Realm name**, type a name.

3 Select **One Source** and then click **Add.**

4 In **Authentication type**, select **SafeWord authentication** and click **OK**.

5 For the **Primary SafeWord server Settings**, enter the following settings:
- In **IP Address**, type the IP address of the SafeWord server.
- In **Port**, type the port number for the SafeWord RADIUS server. The default is 1812. This port must match the number you configured on the RADIUS server.
- In **Server Secret**, enter a RADIUS shared secret.

6 The shared secret must match what is configured on the RADIUS server.

7 If there is a second SafeWord server, configure the settings in **Secondary SafeWord Server Settings**.

To disable Firebox SSL VPN Gateway authentication

On the **Global Cluster Policies** tab, under **Advanced Options**, clear **Enable Portal Page Authentication**.

SafeWord PremierAccess Authorization

If you are using SafeWord PremierAccess for authentication, you can use the following authorization types:

- LDAP
- Local user list
- RADIUS
- No authorization

To configure LDAP authorization, see "To configure LDAP authorization" on page 77.

Using SafeWord for Citrix or SafeWord RemoteAccess for Authentication

Both Safeword for Citrix and SafeWord RemoteAccess use Microsoft's Internet Authentication Server (IAS) to provide RADIUS authentication service to the Firebox SSL VPN Gateway. The IAS RADIUS server receives authentication requests from the Firebox SSL VPN Gateway and sends the user's credentials to SafeWord for verification using an installed SafeWord agent for IAS. Multiple instances of IAS (with the SafeWord agent for IAS) can be deployed for redundancy.

If you are already using SafeWord for Citrix or SafeWord RemoteAccess in your configuration to authenticate using the Web Interface, you need to do the following:

- Install and configure the SafeWord IAS Agent
- Configure the IAS RADIUS server to recognize the Firebox SSL VPN Gateway as a RADIUS client
- Configure the Firebox SSL VPN Gateway to send RADIUS authentication requests to the IAS RADIUS server

To install and configure the IAS Agent and the IAS RADIUS server, see the SafeWord for Citrix or SafeWord Remote Access product documentation.

If you are not currently using SafeWord for Citrix or SafeWord RemoteAccess, you should first install one of these servers following the product documentation.

To configure the Firebox SSL VPN Gateway to send RADIUS authentication requests to the IAS RADIUS server, follow the instructions in "Using RADIUS Servers for Authentication and Authorization" on page 69.

To configure the IAS RADIUS realm

1 Click the **Authentication** tab.

2 In **Realm Name**, type a name for the authentication realm that you will create, select **One Source**, and then click **Add**.

3 In **Select Authentication Type**, in **Authentication Type,** select **RADIUS Authentication** and click **OK**.

4 On the **Authentication** tab, in **Server IP Address**, type the IAS RADIUS server IP address.

5 In **Server Port**, type the IAS RADIUS server port. The default port numbers are 1812 and 1645.

6 In **Server Secret**, type a RADIUS share secret.

Note

Make sure you use a strong shared secret. A strong shared secret is one that is at least eight characters and includes a combination of letters, numbers, and symbols.

7 If there is a secondary IAS RADIUS server, configure the settings for the server in **Secondary Radius Server**.

The RADIUS port number and the RADIUS server secret configured on the Firebox SSL VPN Gateway must match those configured on the IAS RADIUS server.

Using RADIUS Servers for Authentication and Authorization

You can configure the Firebox SSL VPN Gateway to authenticate user access with one or more RADIUS servers. For each RADIUS realm that you use for authentication, you can configure both primary and secondary RADIUS servers. If the primary RADIUS server is unavailable, the Firebox SSL VPN Gateway attempts to authenticate against the secondary RADIUS server for that realm.

If a user is not located on the RADIUS servers or fails authentication, the Firebox SSL VPN Gateway checks the user against the user information stored locally on the Firebox SSL VPN Gateway if the **Enable Local Database lookup** check box is selected on the **Settings** tab of the realm.

The Firebox SSL VPN Gateway software also includes RADIUS authorization, which is configured using Remote Access Policy in Microsoft Internet Authentication Service (IAS). During configuration of the Firebox SSL VPN Gateway, the following information needs to be provided:

- Vendor ID is the vendor-specific code number that was entered in IAS.

- Type is the vendor-assigned attribute number.
- Attribute name is the type of attribute name that is defined in IAS. The default name is CTXSUserGroups=.
- Separator is defined if multiple user groups are included in the RADIUS configuration. A separator can be a space, a period, a semicolon, or a colon.

To configure IAS so the Firebox SSL VPN Gateway can use RADIUS authorization, follow the steps below. These steps assume that IAS is installed from the Add/Remove Programs Control Panel. For more information about installing IAS, see Windows Help.

To configure Microsoft Internet Authentication Service for Windows 2000 Server

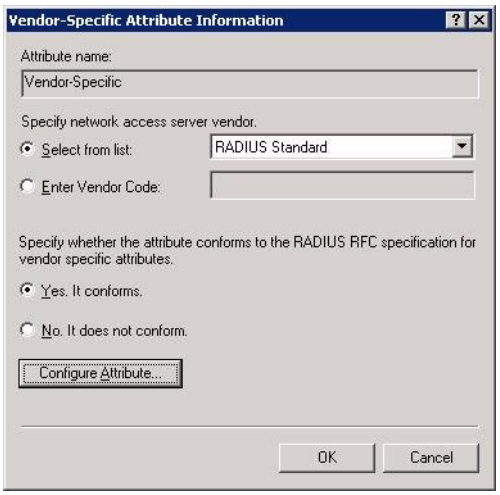
1 Open the Microsoft Management Console (MMC) by clicking **Start > Run**.
2 In **Open**, type **MMC**.
3 In the MMC console, on the **File** menu, click **Add/Remove Snap-in**.
4 Click **Add** and in the **Add/Remove Snap-in** dialog box, select **Internet Authentication Service** and click **Add**.
5 Select **Local computer** and click **Finish**.
6 Click **Close** and then click **OK**.
7 Right-click **Remote Access Policies** and then click **New Remote Access Policy**.
8 Select **Set up a custom policy**.
9 In **Policy name**, give the policy a name and click **Next**.
10 Under **Policy Conditions**, click **Add**, select **Windows-Groups**, and click **Add**.
11 In **Select Groups**, click **Add**, and then type the name of the group.
12 A summary of conditions to match the policy is shown. To add more conditions, click **Add**, otherwise, click **Next**.
13 In the **Edit Dial-In Profile** dialog box, on the **Authentication** tab, select **Encrypted Authentication (CHAP)** and **Unencrypted Authentication (PAP, SPAP)**.

Note

Password Authentication Protocol (PAP) is an authentication protocol that allows Point-to-Point Protocol (PPP) peers to authenticate one another. PAP passes the password and host name or user name unencrypted. PAP does not prevent unauthorized access but identifies the remote end.

14 Clear **Microsoft Encrypted Authentication version 2 (MS-CHAP v2)** and **Microsoft Encrypted Authentication (MS-CHAP)**.
15 Click **OK**.
The Firebox SSL VPN Gateway needs the Vendor-Specific Attribute to match the users defined in the group on the server with those on the Firebox SSL VPN Gateway. This is done by sending the Vendor-Specific Attributes to the Firebox SSL VPN Gateway.
16 In the **Edit Dial-in Profile** dialog box, click the **Advanced** tab.
17 Click **Add**.

18 In the **Add Attributes** dialog box, select **Vendor-Specific** and click **Add**.



19 In the **Vendor-Specific Attribute Information** dialog box, choose **Select from list** and accept the default **RADIUS=Standard**.

The Firebox SSL VPN Gateway needs the Vendor-Specific Attribute to match the users defined in the group on the server with those on the Firebox SSL VPN Gateway.

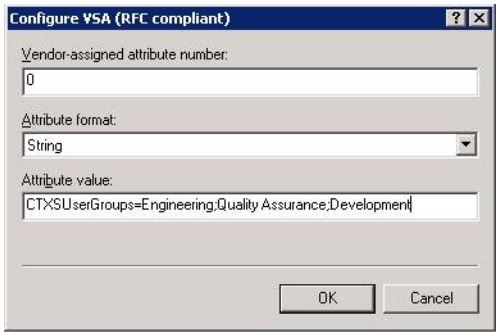
This is done by sending the Vendor-Specific Attributes to the Firebox SSL VPN Gateway

20 The RADIUS default is 0. When configuring RADIUS authorization on the Firebox SSL VPN Gateway, in the field **Vendor Code**, use this default number.

21 Click **Yes. It conforms** and then click **Configure Attribute**.

22 Under **Vendor-assigned attribute number**, type **0**.

This is the assigned number for the User Group attribute. The attribute is in string format. The default is 0.



23 In **Attribute format**, select **String**.

24 In **Attribute value**, type the attribute name and the groups.

For the Firebox SSL VPN Gateway, the attribute value is CTXSUserGroups=*groupname*. If two groups are defined, such as sales and finance, the attribute value is CTXSUserGroups=sales;finance. Separate each group with a semicolon.

25 Click **OK**.

26 In the **Edit Dial-in Profile** dialog box, remove all the other entries, leaving the one that says **Vendor-Specific**.

27 Click **OK**.

When you are finished configuring the Remote Access Policy in IAS, go to the Firebox SSL VPN Gateway and configure the RADIUS authentication and authorization.

To specify RADIUS server authentication

1 Click the **Authentication** tab.

2 In **Realm Name**, type a name for the authentication realm that you will create, select **One Source**, and then click **Add**.

If your site has multiple authentication realms, use a name that identifies the RADIUS realm for which you will specify settings. Realm names are case-sensitive and can contain spaces.

Note

If you want the Default realm to use RADIUS authentication, remove the Default realm as described in "Changing the Authentication Type of the Default Realm" on page 65.

3 In **Select Authentication Type**, choose **RADIUS Authentication** and click **OK**.

The dialog box for the authentication realm opens.

4 In **Server IP Address**, type the IP address of the RADIUS server.

5 In **Server Port**, type the port number. The default port number is 1812.

6 In **Server Secret**, type the RADIUS server secret.

The server secret is configured manually on the RADIUS server and on the Firebox SSL VPN Gateway.

7 If you use a secondary RADIUS server, enter its IP address, port, and server secret.

Note

Make sure you use a strong shared secret. A strong shared secret is one that is at least eight characters and includes a combination of letters, number, and symbols.

To configure RADIUS authorization

1 Click the **Authorization** tab and in **Authorization Type,** select **RADIUS Authorization**.

You can use the following authorization types with RADIUS authentication:

- RADIUS authorization
- Local authorization
- LDAP authorization
- No authorization

2 Complete the settings using the attributes defined in IAS.

For more information about the values for these fields, see "To configure Microsoft Internet Authentication Service for Windows 2000 Server" on page 70.

3 Click **Submit.**

Choosing RADIUS Authentication Protocols

The Firebox SSL VPN Gateway supports implementations of RADIUS that are configured to use the Password Authentication Protocol (PAP) for user authentication. Other authentication protocols such as the Challenge-Handshake Authentication Protocol (CHAP) are not supported.

If your deployment of Firebox SSL VPN Gateway is configured to use RADIUS authentication and your RADIUS server is configured to use PAP, you can strengthen user authentication by assigning a strong shared secret to the RADIUS server. Strong RADIUS shared secrets consist of random sequences of uppercase and lowercase letters, numbers, and punctuation and are at least 22 keyboard characters long. If possible, use a random character generation program to determine RADIUS shared secrets.

To further protect RADIUS traffic, assign a different shared secret to each Firebox SSL VPN Gateway appliance. When you define clients on the RADIUS server, you can also assign a separate shared secret to each client. If you do this, you must configure separately each Firebox SSL VPN Gateway realm that uses

RADIUS authentication. If you synchronize configurations among several Firebox SSL VPN Gateway appliances in a cluster, all the appliances are configured with the same secret. Shared secrets are configured on the Firebox SSL VPN Gateway when a RADIUS realm is created.

Using LDAP Servers for Authentication and Authorization

You can configure the Firebox SSL VPN Gateway to authenticate user access with an LDAP server. If a user is not located in an LDAP directory or fails authentication on a server, the Firebox SSL VPN Gateway checks the user against the user information stored locally on the Firebox SSL VPN Gateway.

LDAP authorization requires identical group names in Active Directory, on the LDAP server, and on the Firebox SSL VPN Gateway. The characters and case must also be the same.

LDAP authentication

Starting with Version 5.0 of the Firebox SSL VPN Gateway, LDAP authentication, by default, is secure using SSL/TLS. There are two types of secure LDAP connections. With one type, the LDAP server accepts the SSL/TLS connection on a port separate from the port used to accept clear LDAP connections. After a client establishes the SSL/TLS connection, LDAP traffic can be sent over the connection. The second type allows both unsecure and secure LDAP connections and is handled by a single port on the server. In this scenario, to create a secure connection, the client first establishes a clear LDAP connection. Then, the LDAP command StartTLS is sent to the server over the connection. If the LDAP server supports StartTLS, the connection is converted to a secure LDAP connection using TLS.

The standard port numbers for unsecure LDAP connections is 389. The port number for secure LDAP connections with SSL/TLS is 636. LDAP connections that use the StartTLS command use port number 389. The Microsoft port numbers for unsecure and secure LDAP connections are 3268 and 3269. If port numbers 389 or 3268 are configured on the Firebox SSL VPN Gateway, it tries to use StartTLS to make the connection. If any other port number is used, connection attempts are made using SSL/TLS.

When configuring the Firebox SSL VPN Gateway to use LDAP authentication and the check box **Allow Unsecure Traffic** is selected, LDAP connections are unsecure.

Note

When upgrading the Firebox SSL VPN Gateway from an earlier version, and an LDAP realm is already configured, LDAP connections are unsecure by default. If this is a new installation of the Firebox SSL VPN Gateway, or you are creating a new LDAP realm, LDAP connections are secure by default.

When configuring the LDAP server, the letter case must match what is on the server and what is on the Firebox SSL VPN Gateway. If the root directory of the LDAP server is specified, all of the subdirectories are also searched to find the user attribute. In large directories, this can affect performance; we recommend that you use a specific organizational unit (OU).

The following table contains examples of user attribute fields for LDAP servers.

LDAP Server	User Attribute	Case Sensitive
Microsoft Active Directory Server	sAMAccountName	No
Novell eDirectory	cn	Yes
IBM Directory Server	uid	
Lotus Domino	CN	
Sun ONE directory (formerly iPlanet)	uid or cn	Yes

This table contains examples of the base dn

Microsoft Active Directory Server	DC=citrix, DC=local
Novell eDirectory	dc=citrix,dc=net
IBM Directory Server	
Lotus Domino	OU=City, O=Citrix, C=US
Sun ONE directory (formerly iPlanet)	ou=People,dc=citrix,dc=com

The following table contains examples of bind dn:

Microsoft Active Directory Server	CN=Administrator, CN=Users, DC=citrix, DC=local
Novell eDirectory	cn=admin, dc=citrix, dc=net
IBM Directory Server	
Lotus Domino	CN=Notes Administrator, O=Citrix, C=US
Sun ONE directory (formerly iPlanet)	uid=admin,ou=Administrators, ou=TopologyManagement,o=NetscapeRoot

Note

For further information to determine the LDAP server settings, see "Determining Attributes in your LDAP Directory" on page 78.

To configure LDAP authentication

1 Click the **Authentication** tab.

2 In **Realm Name**, type a name for the authentication realm.
If your site has multiple authentication realms, you might use a name that identifies the LDAP realm for which you specify settings. Realm names are case-sensitive and can contain spaces.

Note

If you want the Default realm to use LDAP authentication, remove the Default realm as described in "Changing the Authentication Type of the Default Realm" on page 65.

3 Select **One Source** and click **Add**.

4 In **Select Authentication Type**, in **Authentication Type**, choose **LDAP Authentication** and click **OK**.
The Realm dialog box opens.

5 Click the **Authentication** tab.

6 In **Server IP Address**, type the IP address of the LDAP server.

7 In **Server Port**, type the port number.

The LDAP Server port defaults to 389. If you are using an indexed database, such as Microsoft Active Directory with a Global Catalog, changing the LDAP Server port to 3268 significantly increases the speed of the LDAP queries.

If your directory is not indexed, use an administrative connection rather than an anonymous connection from the Firebox SSL VPN Gateway to the database. Download performance improves when you use an administrative connection.

8 Select **Allow Unsecure Traffic** to allow unsecure LDAP connections.
When this check box is clear, all LDAP connections are secure.

9 In **Administrator Bind DN**, type the Administrator Bind DN for queries to your LDAP directory.

The following are examples of syntax for Bind DN:
"domain/user name"
"ou=administrator,dc=ace,dc=com"
"user@domain.name" (for Active Directory)
"cn=Administrator,cn=Users,dc=ace,dc=com"

For Active Directory, the group name specified as cn=*groupname* is required. The group name that is defined in the Firebox SSL VPN Gateway must be identical to the group name that is defined on the LDAP server.

For other LDAP directories, the group name either is not required or, if required, is specified as ou=*groupname*.

The Firebox SSL VPN Gateway binds to the LDAP server using the administrator credentials and then searches for the user. After locating the user, the Firebox SSL VPN Gateway unbinds the administrator credentials and rebinds with the user credentials.

10 In **Administrator Password**, type the password.

11 In **Base DN (where users are located),** type the Base DN under which users are located.

Base DN is usually derived from the Bind DN by removing the user name and specifying the group where users are located. Examples of syntax for Base DN:
"ou=users,dc=ace,dc=com"
"cn=Users,dc=ace,dc=com"

12 In **Server login name attribute**, type the attribute under which the Firebox SSL VPN Gateway should look for user logon names for the LDAP server that you are configuring. The default is sAMAccountName. If you are using other directories, use cn.

13 Click **Submit**.

If a user is not located in an LDAP directory or fails authentication on a server, the Firebox SSL VPN Gateway checks the user against the user information stored locally on the Firebox SSL VPN Gateway.

LDAP authorization requires identical group names in Active Directory, on the Firebox SSL VPN Gateway, and on the LDAP server. The characters and case must also be the same.

Note

For further information to determine the LDAP server settings, see "Determining Attributes in your LDAP Directory" on page 78.

LDAP Authorization

The following is a discussion of LDAP group memberships attributes that will and will not work with Firebox SSL VPN Gateway authorization.

You can use the following authorization types with LDAP authentication:

- Local authorization
- LDAP authorization
- No authorization

If you are using double-source authentication, authorization is based on the primary authentication method, not the secondary authentication method.

Group memberships from group objects working evaluations

LDAP servers that evaluate group memberships from group objects indirectly work with Firebox SSL VPN Gateway authorization.

Some LDAP servers enable user objects to contain information about groups to which they belong, such as Active Directory or eDirectory. A user's group membership can be computable attributes from the user object, such as IBM Directory Server or Sun ONE directory server. In some LDAP servers, this attribute can be used to include a user's dynamic group membership, nesting group membership, and static group membership to locate all group memberships from a single attribute.

For example, in IBM Directory Server, all group memberships, including the static, dynamic, and nested groups, can be returned using the ibm-allGroups attribute. In Sun ONE, all roles, including managed, filtered, and nested, are calculated using the nsRole attribute.

Group memberships from group objects non-working evaluations

LDAP servers that evaluate group memberships from group objects indirectly will not work with Firebox SSL VPN Gateway authorization.

Some LDAP servers enable only group objects such as the Lotus Domino LDAP server to contain information about users. The LDAP server does not enable the user object to contain information about groups. For this type of LDAP server, group membership searches are performed by locating the user on the member list of groups.

LDAP authorization group attribute fields

The following table contains examples of LDAP group attribute fields.

Microsoft Active Directory Server	memberOf
Novell eDirectory	groupMembership
IBM Directory Server	ibm-allGroups
Sun ONE directory (formerly iPlanet)*	nsRole

To configure LDAP authentication

1 Click the **Authentication** tab.

2 In **Realm Name**, type a name for the authentication realm that you will create, select **One Source**, and then click **Add**.

If your site has multiple authentication realms, you might use a name that identifies the LDAP realm for which you will specify settings. Realm names are case-sensitive and can contain spaces.

Note

If you want the Default realm to use LDAP authentication, remove the Default realm as described in "Changing the Authentication Type of the Default Realm" on page 65.

3 In **Select Authentication Type**, choose **LDAP Authentication** and click **OK**.

The Realm dialog box opens.

4 Click the **Authentication** tab.

5 In **Server IP Address**, type the IP address of the LDAP server.

6 In **Server Port**, type the port number.

The LDAP Server port defaults to 389. If you are using an indexed database, such as Microsoft Active Directory with a Global Catalog, changing the LDAP Server port to 3268 significantly increases the speed of the LDAP queries.

If your directory is not indexed, use an administrative connection rather than an anonymous connection from the Firebox SSL VPN Gateway to the database. Download performance improves when you use an administrative connection.

7 In **Administrator Bind DN**, type the Administrator Bind DN for queries to your LDAP directory.

The following are examples of syntax for Bind DN:
"domain/user name"
"ou=administrator,dc=ace,dc=com"
"user@domain.name" (for Active Directory)
"cn=Administrator,cn=Users,dc=ace,dc=com"

For Active Directory, the group name specified as cn=*groupname* is required. The group name that is defined in the Firebox SSL VPN Gateway must be identical to the group name that is defined on the LDAP server.

For other LDAP directories, the group name either is not required or, if required, is specified as ou=*groupname*.

The Firebox SSL VPN Gateway binds to the LDAP server using the administrator credentials and then searches for the user. After locating the user, the Firebox SSL VPN Gateway unbinds the administrator credentials and rebinds with the user credentials.

8 In **Administrator Password**, type the password.

9 In **Base DN (where users are located),** type the Base DN under which users are located.

Base DN is usually derived from the Bind DN by removing the user name and specifying the group where users are located. Examples of syntax for Base DN:
"ou=users,dc=ace,dc=com"
"cn=Users,dc=ace,dc=com"

10 In **Server login name attribute** type the attribute under which the Firebox SSL VPN Gateway should look for user logon names for the LDAP server that you are configuring. The default is sAMAccountName. If you are using other directories, use cn.

11 Click **Submit**.

After configuring LDAP authentication, configure LDAP authorization.

To configure LDAP authorization

1 Click the **Authorization** tab.

2 In **LDAP Server IP Address**, type the IP address of the LDAP server.

3 In **LDAP Server Port**, type the port number. The default port number is 389.

4 In **LDAP Administrator Bind DN**, type the Administrator Bind DN for queries to your LDAP directory.

The following are examples of syntax for Bind DN:
domain/user name
"ou=administrator,dc=ace,dc=com"
"user@domain.name" (for Active Directory)
"cn=Administrator,cn=Users,dc=ace,dc=com"

For Active Directory, the group name specified as cn=*groupname* is required. The group name that is defined in the Firebox SSL VPN Gateway must be identical to the group name that is defined on the LDAP server.

For other LDAP directories, the group name either is not required or, if required, is specified as ou=*groupname*.

The Firebox SSL VPN Gateway binds to the LDAP server using the administrator credentials and then searches for the user. After locating the user, the Firebox SSL VPN Gateway unbinds the administrator credentials and rebinds with the user credentials.

5 In **LDAP Administrator Password**, type the password.

6 In **LDAP Base DN (where users are located)**, type the Base DN under which users are located.

Base DN is usually derived from the Bind DN by removing the user name and specifying the group where users are located. The following are examples of syntax for Base DN:
"ou=Users,dc=ace,dc=com"
"cn=Users,dc=ace,dc=com"

7 In **LDAP Server login name attribute**, type the attribute under which the Firebox SSL VPN Gateway should look for user logon names for the LDAP server that you are configuring. The default is cn. If Active Directory is used, type the attribute sAMAccountName.

8 In **LDAP Group Attribute,** type the name of the attribute. The default is "memberOf." This attribute enables the Firebox SSL VPN Gateway to obtain the groups associated with a user during authorization.

9 Click **Submit**.

Using certificates for secure LDAP connections

You can use a secure client certificate with LDAP authentication and authorization. To use a client certificate, you must have an enterprise Certificate Authority, such as Certificate Services in Windows Server 2003, running on the same computer that is running Active Directory. You can create a client certificate using the Certificate Authority.

To use a client certificate with LDAP authentication and authorization, it must be a secure certificate using SSL. Secure client certificates for LDAP are uploaded to the Firebox SSL VPN Gateway.

To upload a secure client certificate for LDAP

1 On the **VPN Gateway Cluster** tab, click the **Administration** tab.

2 Next to **Upload Private Key + Client Certificate for LDAP**, click **Browse**.

3 Navigate to the client certificate and click **Open**.

Determining Attributes in your LDAP Directory

If you need help determining your LDAP Directory attributes, you can easily look them up with the free LDAP Browser from Softerra.

To install and set up the LDAP Browser

1 Download the free LDAP Browser application from the Softerra LDAP Administrator Web site http://www.ldapbrowser.com.

2 Install LDAP Browser and open it.

3 From the LDAP Browser window, choose **File > New Profile** and specify the following settings:

Host

Host name or IP address of your LDAP server.

Port

Defaults to 389.

Base DN

You can leave this field blank. (The information provided by the LDAP Browser will help you determine the Base DN needed for the Authentication tab.)

Anonymous Bind

Select the check box if the LDAP server does not require credentials to connect to it. If the LDAP server requires credentials, leave the check box cleared, click **Next**, and enter the credentials.

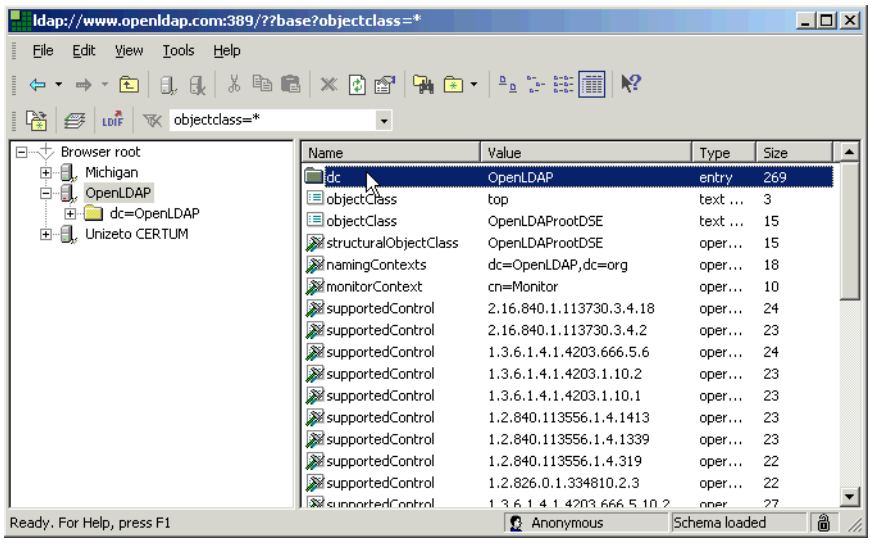
4 Click **Finish**.

The LDAP Browser displays the profile name that you just created in the left pane of the LDAP Browser window and connects to the LDAP server.

To look up LDAP attributes

1 In the left pane of the LDAP Browser, select the profile name that you created.

2 To look up the Base DN, in the right pane, locate the namingContexts attribute. The value of that attribute is the Base DN for your site. The Base DN is typically dc=myDomain,dc=com (if your directory tree is based on Internet domain names) or ou=domain,o=myOrg,c=country.



3 Navigate through the browser to locate other attributes.

Using RSA SecurID for Authentication

If your site uses an RSA ACE/Server and SecurID for authentication, you can configure the Firebox SSL VPN Gateway to authenticate user access with the
RSA ACE/Server. The Firebox SSL VPN Gateway acts as an RSA Agent Host, authenticating on behalf of the users who use Secure Access to log on. The Firebox SSL VPN Gateway supports the use of one RSA ACE/Server.

The Firebox SSL VPN Gateway supports RSA ACE/Server Version 5.2 and higher. The Firebox SSL VPN Gateway also supports replication servers. Replication server configuration is completed on the RSA ACE/Server and is part of the sdconf.rec file that is uploaded to the Firebox SSL VPN Gateway. If this is configured on the RSA ACE/Server, the Firebox SSL VPN Gateway attempts to connect to the replication servers if there is a failure or network connection loss with the primary server.

Note

If you are running a RADIUS server on an RSA server, configure RADIUS authentication as described in "Using RADIUS Servers for Authentication and Authorization" on page 69.

If a user is not located on the RSA ACE/Server or fails authentication on that server, the Firebox SSL VPN Gateway checks the user against the user information stored locally on the Firebox SSL VPN Gateway, if the check box **Use the local user database on the Access Gateway** is checked on the **Settings** tab.

The Firebox SSL VPN Gateway supports Next Token Mode. If a user enters three incorrect passwords, the Secure Access Client prompts the user to wait until the next token is active before logging on. If a user logs on too many times with an incorrect password, the RSA server might disable the user's account.

To contact the RSA ACE/Server, the Firebox SSL VPN Gateway must include a copy of the ACE Agent Host sdconf.rec configuration file that is generated by the RSA ACE/Server. The following procedures describe how to generate and upload that file.

Note

The following steps describe the required settings for the Firebox SSL VPN Gateway. Your site might have additional requirements. Refer to the RSA ACE/ Server documentation for more information.
If the Firebox SSL VPN Gateway needs to be imaged again, see "Resetting the node secret" on page 82.

To generate a sdconf.rec file for the Firebox SSL VPN Gateway

1. On the computer where your RSA ACE/Server Administration interface is installed, go to **Start > Programs > RSA ACE Server > Database Administration - Host Mode**.
2. In the RSA ACE/Server Administration interface, go to **Agent Host > Add Agent Host** (or, if you are changing an Agent Host, **Edit Agent Host**).
3. In the **Name** field, enter a descriptive name for the Firebox SSL VPN Gateway (the Agent Host for which you are creating a configuration file).
4. In the **Network address** field, enter the internal Firebox SSL VPN Gateway IP address.
5. For **Agent type**, select **UNIX Agent**.
6. Make sure that the **Node Secret Created** check box is clear and inactive when you are creating an Agent Host. The RSA ACE/Server sends the Node Secret to the Firebox SSL VPN Gateway the first time that it authenticates a request from the Firebox SSL VPN Gateway. After that, the Node Secret Created check box is selected. By clearing the check box and generating and uploading a new configuration file, you can force the RSA ACE/Server to send a new Node Secret to the Firebox SSL VPN Gateway.
7. Indicate which users can be authenticated through the Firebox SSL VPN Gateway through one of the following methods:
   - To configure the Firebox SSL VPN Gateway as an open Agent Host, click **Open to All Locally Known Users** and then click **OK**.
   - To select the users to be authenticated, click **OK**, go to **Agent Host > Edit Agent Host**, select the Firebox SSL VPN Gateway host, and then click **OK**. In the dialog box, click the **User Activations** button and select the users.

8 To create the configuration file for the new or changed Agent Host, go to **Agent Host > Generate Configuration Files**.
The file that you generate (sdconf.rec) is what you will upload to the Firebox SSL VPN Gateway, as described in the next procedure.

Enable RSA SecurID authentication for the Firebox SSL VPN Gateway

You can use the following authorization types with RSA SecureID authentication:

- RSA authorization
- Local authorization
- LDAP authorization
- No authorization

To enable RSA SecurID authentication

1 Click the **Authentication** tab.

2 In **Realm Name**, type a name to identify the RSA ACE/Server. Realm names are case-sensitive and can contain spaces.

3 Select **One Source** and click **Add**.

Note

If you want the Default realm to use RSA authentication, remove the Default realm as described in "Changing the Authentication Type of the Default Realm" on page 65.

4 In the **Select Authentication Type** dialog box, in **Authentication Type**, select **RSA SecurID Authentication**.

5 Click **OK**.
A dialog box for the authentication realm opens.

6 To upload the sdconf.rec file that you generated in the previous procedure, on the **Authentication tab**, click **Upload sdconf.rec file** and use the dialog box to locate and upload the file.
The sdconf.rec file is typically written to ace\data\config_files and to windows\system32.

Note

If an invalid sdconf.rec file is uploaded to the Firebox SSL VPN Gateway, it might cause the Firebox SSL VPN Gateway to send out messages to non-existent IP addresses. This might be flagged in a network monitor as network spamming.

- The file status message indicates whether or not an sdconf.rec file was uploaded. If one was uploaded and you need to replace it, click **Upload sdconf.rec file** and use the dialog box to locate and upload the file.
- The first time that a client is successfully authenticated, the RSA ACE/Server writes some configuration files to the Firebox SSL VPN Gateway. If you subsequently change the IP address of the Firebox SSL VPN Gateway, click **Remove ACE Configuration Files**, restart when prompted, and then upload a new sdconf.rec file.

7 To use LDAP for authorization, click the **Authorization** tab and complete the settings.
For more information about LDAP settings, see "Using LDAP Servers for Authentication and Authorization" on page 73. For looking up LDAP server settings, see "Determining Attributes in your LDAP Directory" on page 78.

8 Click **Submit**.

Configuring RSA Settings for a Cluster

If you have two or more appliances configured as a cluster, the sdconf.rec file needs to contain the FQDNs of all the appliances. The sdconf.rec file is installed on one Access Gateway and then published. This allows all of the appliances to connect to the RSA server.

You can also limit connections to the RSA server from user connections. For example, you have three appliances in your cluster. If the FQDNs of the first and second appliances are included in the sdconf.rec file and the third appliance is not, users can connect only to the RSA server using the first two appliances.

Resetting the node secret

If you reimaged the Firebox SSL VPN Gateway, giving it the same IP address as before, and restored your configuration, you must also reset the node secret on the RSA ACE/Server. Because the Firebox SSL VPN Gateway was reimaged, the node secret no longer resides on it and an attempt to authenticate with the RSA ACE/Server fails.

After you reset the server secret on the RSA ACE/Server, the next authentication attempt prompts the RSA ACE/Server to send a node secret to the Firebox SSL VPN Gateway.

To reset the node secret on the RSA ACE/Server

1 On the computer where your RSA ACE/Server Administration interface is installed, go to **Start > Programs > RSA ACE Server > Database Administration - Host Mode**.

2 In the RSA ACE/Server Administration interface, go to **Agent Host > Edit Agent Host**.

3 Select the Firebox SSL VPN Gateway IP address from the list of agent hosts.

4 Clear the **Node Secret Created** check box and save the change.

5 The RSA server sends the node secret on the next authentication attempt from the Firebox SSL VPN Gateway.

Configuring Gemalto Protiva Authentication

Protiva is a strong authentication platform that was developed to use the strengths of Gemalto's smart card authentication. With Protiva, users log on with a user name, password, and one-time password generated by the Protiva device. Similar to RSA SecurID, the authentication request is sent to the Protiva Authentication Server and the password is either validated or rejected.

To configure Gemalto Protiva to work with the Access Gateway, use the following guidelines:

- Install the Protiva server.
- Install the Protiva Internet Authentication Server (IAS) agent plug-in on a Microsoft IAS RADIUS server. Make sure you note the IP address and port number of the IAS server
- Configure a realm on the Access Gateway to use RADIUS authentication and enter the settings of the Protiva server.

To configure a Gemalto Protiva realm

1 In the Administration Tool, click the **Authentication** tab.

2 Under **Add an Authentication Realm**, in **Realm name**, type a name.

3 Select **One Source** and then click **Add**.

Note

Note: If you are configuring double-source authentication, click **Two Source** and then click **Add**. For more information about configuring double-source authentication, see "Configuring Double-Source Authentication" on page 85.

4 In **IP address** type the IP address of the RADIUS IAS server.

5 In **Port**, type the port number.

6 In **Server secret**, type the node secret of the RADIUS IAS server.

7 Select **Use the password one time** and click **Submit**

Configuring NTLM Authentication and Authorization

You can configure the Firebox SSL VPN Gateway to use Windows NT LAN Manager (NTLM) authentication to authenticate users against the user database on a Windows NT 4.0 domain controller.

If a user is not located in the user database on the Windows NT 4.0 domain controllers, or fails authentication, the Firebox SSL VPN Gateway can check for the user name in the Local Users list on the Firebox SSL VPN Gateway and authenticate the user against the local list if **Use the local user database on the** Firebox SSL VPN **Gateway** check box is selected on the **Settings** tab.

A Windows NT 4.0 domain controller maintains domain user accounts in a database on the Windows NT 4.0 server. A domain user account includes a user name and password and other information about the user.

To configure NTLM authentication, you create an NTLM authentication realm that includes the address and port that the Firebox SSL VPN Gateway uses to connect to the Windows NT 4.0 domain controller. You also specify a time-out value in which an authentication attempt to the server must complete.

When a user logs on to the Firebox SSL VPN Gateway, the user enters the user name and password maintained in the domain user account on the Windows NT 4.0 server.

The Firebox SSL VPN Gateway connects to the Windows NT 4.0 server and passes these credentials to the server. The server authenticates the user.

To configure NTLM authentication

1 Click the **Authentication** tab.

2 Under **Add an Authentication Realm**, in **Realm name**, type a name for the authentication realm.
If your site has multiple authentication realms, you might use a name that identifies the NTLM realm for which you specify settings. Realm names are case-sensitive and can contain spaces.

Note

Note: If you want the Default realm to use NTLM authentication, remove the Default realm as described in "To remove and create a Default realm" on page 70.

3 Select **One Source** and click **Add**.

4 In **Select Authentication Type**, in **Authentication type**, choose **NTLM authentication** and click **OK**.
The Realm dialog box opens.

5 Click the **Authentication** tab.

6 In **IP Address or FQDN**, type the IP address of the Windows NT 4.0 domain controller.

7 In **Port**, type the port number on which the Windows NT 4.0 domain controller listens for the NTLM authentication connection.
The default port entry for NTLM authentication connections is 139.

Note

Note: When 0 (zero) is entered as the port, the Access Gateway attempts to automatically detect a port number for this connection.

8 In **Time-out (in seconds)**, enter the number of seconds within which the authentication attempt must complete. If the authentication does not complete within this time interval, it fails.

9 Click **Submit**.

Configuring NTLM Authorization

A Windows NT 4.0 domain controller maintains group accounts. A group account is a collection of individual user domain accounts (and other accounts).

To configure NTLM authorization, you click the **Authorization** tab in the authentication realm and enter the address and port that the Firebox SSL VPN Gateway uses to connect to the Windows NT 4.0 domain controller. You also specify a time-out value in which an authorization attempt to the Windows NT server must complete.

After a user successfully authenticates, the domain controller returns to the Firebox SSL VPN Gateway a list of all global groups of which the authenticated user is a member.

The Firebox SSL VPN Gateway then looks for a user group name on the Firebox SSL VPN Gateway that matches the name of a Windows NT 4.0 global group to which the user belongs. If the Firebox SSL VPN Gateway finds a match, the user is granted the authorization privileges to the internal networks that are associated with the user group on the Firebox SSL VPN Gateway.

To configure NTLM authorization

1 Click the **Authentication** tab and open the authentication realm for which you want to enable NTLM authorization.

2 Click the **Authorization** tab.

3 In **Authorization type**, select **NTLM authorization**.

4 In **Server IP Address or FQDN**, type the FQDN or IP address of the Windows NT 4.0 domain controller that will perform the NTLM authorization.

5 In **Server Port**, type the port number.
The default port entry for NTLM authentication connections is 139.

Note

Note: When 0 (zero) is entered as the port, the Firebox SSL VPN Gateway attempts to automatically detect a port number for this connection.

6 In **Timeout (in seconds)**, enter the number of seconds within which the authorization attempt must complete before the authentication attempt is abandoned.

7 Click **Submit**.

Configuring Authentication to use One-Time Passwords

If authentication on the Firebox SSL VPN Gateway is configured to use a one-time password with RADIUS, such as provided by an RSA SecurID token, the Firebox SSL VPN Gateway attempts to reauthenticate users using the cached password. This occurs when changes are made to the Firebox SSL VPN Gateway using the Administration Tool or if the connection between the Secure Access Client and the Firebox SSL VPN Gateway is interrupted and then restored.

You can prevent the storage of one-time passwords in cache, which forces the user to enter their credentials again.

To prevent caching of one-time passwords

1 In the Administration Tool, click the **Authentication** tab.

2 Open the authentication realm that uses the one-time password.

3 Select **Use the password one time** and click **Submit**.

Configuring Double-Source Authentication

The Firebox SSL VPN Gateway supports double-source authentication. On the **Authentication** tab, you can configure two types of authentication, such as LDAP and RSA SecurID for one realm. When users log on to the Firebox SSL VPN Gateway using a Web browser, and double-source authentication is configured, they are redirected automatically to a logon Web portal page. There, they type in their user name and passwords for each type of authentication. If they are using the Secure Access Client to log on, the Secure Access dialog box appears requesting the same information as the Web page.

There can be a mix of double-source authentication realms. For example, you can have one or more realms for single authentication and then have one or more realms configured for double-source authentication. In a mixed authentication environment, when users log on using either the Web browser or Secure Access Client, they will see two password fields. If they are logging on using only one authentication method, the second password field is left blank.

For more information about logging on using the Web-based portal page, see "Double-source Authentication Portal Page" on page 43.

To create and configure a double-source authentication realm

1 On the **Authentication** tab, click **Authentication**.

2 In **Realm Name**, type a name.

3 Select **Two Source** and then click **Add**.

4 In the **Select Authentication Type** dialog box, select the authentication types in **Primary Authentication Type** and **Secondary Authentication Type**.

5 Click **Add**.

6 On the **Primary Authentication** tab, configure the settings for the first authentication type and click **Submit**.

7 On the **Secondary Authentication** tab, configure the settings for the second authentication type and click **Submit**.

8 On the **Authorization** tab, in **Authorization Type**, select the authorization type you want to use, configure the settings, and click **Submit**.

Double-source authentication works in reverse of how it is configured on the Firebox SSL VPN Gateway. For example, if you configured RSA SecurID on the **Secondary Authentication** tab and LDAP on the **Primary Authentication** tab, when users log on, they type their LDAP password in the first password field and the RSA SecurID personal identification number (PIN) and passcode in the second password field. When users click **Connect**, the Firebox SSL VPN Gateway authenticates using the RSA SecureID PIN

and passcode first and then the LDAP password second. Whatever is typed in the first password field is done last and the second password field is done first.

Changing Password Labels

You can change the password labels to accurately reflect the authentication type with which the user is logging on and to provide the correct prompt for what the user needs to type. This is useful when the Firebox SSL VPN Gateway is configured to support third-party authentication types. For example, if users are required to authenticate using LDAP and Gemalto protiva strong authentication system (RADIUS), you can change the password labels to reflect what the user needs to type in the fields. Instead of the labels, **Password** and **Secondary Password**, the labels could be **Windows domain password** and **Gemalto protiva passcode**.

The labels can be changed if you are using one-source or double-source authentication.

To change the password labels

1 Click the **Authentication** tab, and under **Add an Authentication Realm**, click **Advanced**.

2 In **Password label** and **Secondary password label**, type the values for the labels.

3 Click **OK**

When users log on, they see the new password labels.

CHAPTER 6

Adding and Configuring Local Users and User Groups

User groups define the resources the user has access to when connecting to the corporate network through the Firebox SSL VPN Gateway. Groups are associated with the local users list. After adding local users, you can then define the resources they have access to on the **Access Policy Manager** tab. This chapter discusses the following group settings:

- Adding Local Users
- User Group Overview
- Creating User Groups
- Configuring Properties for a User Group
- Configuring Resources for a User Group
- Setting the Priority of Groups

Adding Local Users

You can create user accounts locally on the Firebox SSL VPN Gateway to supplement the users on authentication servers. For example, you might want to create local user accounts for temporary users, such as consultants or visitors, without creating an entry for those users on the authentication server. In that case, you add the user to the Firebox SSL VPN Gateway local user list as described in this section.

If you associate more than one group with a user account, the properties of the first group that you select for the user is used.

To create a user on the Firebox SSL VPN Gateway

1 Click the **Access Policy Manager** tab.

2 In the left-pane, right-click **Local Users** and then click **New User**.

3 In **User name**, type a user name. This is the logon name the user needs when logging onto Secure Access. User names can contain spaces.

4 In **Password** and **Verify Password**, type a password for the user in the two fields.
A user enters this password when logging onto Secure Access. A password must be six or more characters up to a maximum of 128 characters. Do not use a forward slash (/) in the user name or password.

5 All users are members of the Default resource group. To add a user to another group, under **Local Users**, click and drag the user to the user group to which you want the user to belong.

To delete a user from the Firebox SSL VPN Gateway

Right-click the user in the **Local Users** list and click **Remove**.

User Group Overview

When you enable authorization on the Firebox SSL VPN Gateway, user group information is obtained from the authentication server after a user is authenticated. If the group name that is obtained from the authentication server matches a group name created locally on the Firebox SSL VPN Gateway, the properties of the local group are used for the matching group obtained from the authentication servers.

Note

Group names on authentication servers and on the Firebox SSL VPN Gateway must be identical and they are case sensitive.

Each user should belong to at least one group that is defined locally on the Firebox SSL VPN Gateway. If a user does not belong to a group, the overall access of the user is determined by the **Deny Access without ACL** setting on the **Global Cluster Policies** tab, as follows:

- If the Deny Access option is enabled, the user cannot establish a connection
- If the Deny Access option is disabled, the user has full network access
- In either case, the user can use kiosk mode, but network access within that session is determined by the **Deny Access without ACL** setting

You can also add local groups that are not related to groups on authentication servers. For example, you might create a local group to set up a contractor or visitor to whom you want to provide temporary access without having to create an entry on the authentication server. For information about creating a local user, see "Adding Local Users" on page 87.

Several aspects of Firebox SSL VPN Gateway operation are configured at the group level. These are separated between group properties and group resources.

Group properties include:

- Groups that inherit properties from the default group.
- Requiring users to log on again if there is a network interruption or if the computer is coming out of standby or hibernate.
- Enabling single sign-on.
- Running logon scrips when a user logs on using domain credentials.
- Denying access to applications to the network that do not have a defined application policy.
- Specify the length of time a session is active. If the user has a 60 minute session time-out, the session ends at 60 minutes. Users are given a one minute warning that their session is about to end.
- Enabling Split DNS allows local DNS servers to be contacted if the DNS servers for the remote client are non-responsive.
- IP pooling where a unique IP address is assigned to each client's session.
- Portal page usage that defines the portal page the user sees when logging on. The portal page can be one of the provided templates, modified for individual companies.
- Requiring client certificates.

Group resources include:

- Network resources that define the networks to which clients can connect.
- Application policies that define the applications users can use when connected. In addition to selecting the application, you can further define which networks the application has access to and if any end point policies need to be met when connecting.
- File share resources that define which file shares the user can connect to when logged on in kiosk mode.
- Kiosk resources that defines how the user can log on, the Web address the user needs, and which file shares and applications the user can use when logged on.
- End point resources and policies that define the required and option parameters that must be on the user's computer when logging on.

If a user belongs to more than one group, group policies are applied to the user based on the group priorities set on the **Group Priority** tab, as described in "Setting the Priority of Groups" on page 106.

Creating User Groups

User groups are created on the **Access Policy Manager** tab. Multiple user groups can be created and configured. When a new group is created, the properties page appears that allows you to configure the settings for the group. You can also add local groups that are not related to groups on authentication servers. After the settings are complete, resources can be added to the group.

Note

If you create a user group that has more than 127 characters and then delete that user group, it still appears on the **Group Priority** tab after deletion. To resolve this problem, user group names should have fewer than 127 characters. Any characters over this limit are truncated.

To create a local user group

1. Click the **Access Policy Manager** tab.
2. In the left pane, right-click **User Groups** and then click **New Group**.
3. In **Group Name**, type a descriptive name for the group, such as "Temp Employees" or "accounting" and then click **OK**.
   A dialog box for the added group appears.

Note

If you want the group's properties to be used for authentication obtained from authentication servers, the group name must match the authentication server group name, including case and use of spaces.

4. To configure the group, see "Configuring Properties for a User Group" on page 90.

To remove a user group

On the **Access Policy Manager** tab, in the left-pane, right-click a group and then click **Delete**.

Configuring Properties for a User Group

Group properties include configuring access, networking, portal pages, and client certificates. Properties are configured by right-clicking a group and then clicking **Properties**. Settings for the group are configured on the **General**, **Networking**, **Gateway Portal**, **Members**, and **Client Certificates** tabs.

Default group properties

If the only group that is configured on the Firebox SSL VPN Gateway is the Default user group, all local users receive the settings configured for this group. You can control access to the Default user group settings by configuring additional groups on the Firebox SSL VPN Gateway and then restricting access to the Default user group.

For example, two users are part of a group for contractors. They are allowed to connect to specific corporate resources, such as an Exchange server and a file server. If they inherit the settings from the Default group, you might have unintentionally configured these users to have access to resources that are only for permanent employees.

You can allow or deny users to inherit the Default group settings in the user group properties. This check box is not available for the Default group.

To enable or disable Default group properties

1 Click the **Access Policy Manager** tab.

2 In the left pane, right-click the user group and then click **Properties.**

3 On the **General** tab, do one of the following:
- To prevent users from inheriting the Default group settings, clear **Inherit properties from the Default Group**
- To allow users to inherit the Default group settings, select **Inherit properties from the Default Group**

4 Click **OK**.

Forcing Users to Log on Again

By default, if a user's network connection is briefly interrupted, the user does not have to log on again when the connection is restored. You can require that users log on after interruptions such as when a computer comes out of hibernate or standby, when the user switches to a different wireless network, or when a connection is forcefully closed.

To force users to log on after a network interruption or on system resume

1 Click the **Access Policy Manager** tab.

2 In the left pane, right-click a group and click **Properties**.

3 On the **General** tab, under **Session Options**, select one or both of the following:
- **Authenticate after network interruption.** This option forces a user to log on again if the network connection is briefly interrupted.
- **Authenticate upon system resume.** This option forces a user to log on again if the user's computer awakens from stand by or hibernate. This option provides additional security for unattended computers.

4 Click **OK**.

Note

If you want to close a connection and prevent a user or group from reconnecting automatically, you must select the Authenticate after network interruption setting. Otherwise, users immediately reconnect without being prompted for their credentials. For more information, see "Managing Client Connections" on page 133.

Configuring Secure Access Client for single sign-on

By default, Windows users open a connection by launching the Secure Access Client from the desktop. You can specify that the Secure Access Client start automatically after the user logs onto Windows by enabling single sign-on. Users' Windows logon credentials are passed to the Firebox SSL VPN Gateway for authentication.

Enable single sign-on only if users' computers are logging on to your organization's domain. If single sign-on is enabled and a user connects from a computer that is not on your domain, the user is prompted to log on.

Note

Users must be logged on as a Power User or be a member of the Power Users group to use single sign-on to Windows.

If the Secure Access Client is configured for single sign-on with Windows, it automatically starts after the user logs on to Windows. The user's Windows logon credentials are passed to the Firebox SSL VPN Gateway for authentication. Enabling single sign-on for the Secure Access Client facilitates operations on the remote computer such as installation scripts and automatic drive mapping

To configure Secure Access Client for single sign-on

1 Click the **Access Policy Manager** tab.

2 In the left pane, right-click a group and then click **Properties**.

3 On the **General** tab, under **Session Options**, click **Enable single sign-on**.

4 Click **OK**.

Note

If you configured double-source authentication, you cannot use single sign-on.

Enabling domain logon scripts

In your network, you may have logon scripts that run on the client computer after a successful log on. If logon scripts are enabled on the Firebox SSL VPN Gateway, after authentication, the Firebox SSL VPN Gateway establishes the connection, obtains Windows logon scripts from the domain controller, and then runs the logon scripts to perform operations such as automatic drive mapping. If the domain controller cannot be contacted, the Firebox SSL VPN Gateway connection is completed but the logon scripts are not run.

Note

Clients that want to use single sign-on to Windows and logon scripts must be logged on as a Power User or be a member of the Power Users group. The Firebox SSL VPN Gateway can run logon scripts that are defined in the user's Windows profile. Logon scripts that are defined in Active Directory are not

supported and do not run. If the domain controller cannot be contacted, the Firebox SSL VPN Gateway connection is completed but the logon scripts are not run.

Note

Important: The client computer must be a domain member in order to run domain logon scripts.

To enable logon scripts

1 Click the **Access Policy Manager** tab.

2 In the left pane, right-click a group and click **Properties**.

3 On the **General** tab, under **Session Options**, select **Run logon scripts**.

4 Click **OK**.

Note

Logon script support is restricted to scripts that are executed by the command processor, such as executables and batch files. Visual Basic and JavaScript logon scripts are not supported.

Enabling session time-out

You can configure the Secure Access Client to force a disconnection with the Firebox SSL VPN Gateway if there is no activity on the connection for a specified number of minutes. One minute before a session times out (disconnects), the user receives an alert indicating the session will close. If the session closes, the user must log on again.

There are three different options when configuring a session time-out value:

- **User session timeout.** If you enable this setting, the Secure Access Client disconnects after the time-out interval elapses regardless of what the user is doing. There is no action the user can take to prevent the disconnection from occurring when the time-out interval elapses.
- **Network inactivity timeout**. If you enable this setting, the Secure Access Client disconnects if no network packets are sent from the client to the Firebox SSL VPN Gateway for the specified interval.
- **Idle session timeout**. If you enable this setting, the user session times out if there is no mouse or keyboard activity on the client for the specified interval.

You can enable any of these settings by entering a value between 1 and 65536 to specify a number of minutes for the time-out interval. You can disable any of these settings by entering a 0 (zero). If you enter a 0, the time-out session is not activated and the setting has no effect on client connections.

If you enable more than one of these settings, the first time-out interval to elapse closes the client connection.

To enable session time-out

1 Click the **Access Policy Manager** tab.

2 In the left pane, right-click a group and then click **Properties**.

3 On the **General** tab, under **Session options**, type the number of minutes in any of these settings:
- User session timeout
- Network inactivity timeout
- Idle session timeout

4 Click **OK**.

Configuring Web Session Time-Outs

When a user is logged on to the Firebox SSL VPN Gateway and using a Web browser to connect to Web sites in the secure network, cookies are set to determine if a user's Web session is still active on the Firebox SSL VPN Gateway. If the Firebox SSL VPN Gateway cookie expires and logon page authentication is enabled, the end user is prompted to enter authentication credentials to resume the Web session. This provides a measure of security for limiting the amount of time network attacks could occur during an unattended Web session.

To enable Web session time-outs

1 Click the **Global Cluster Policies** tab.

2 Under **Access options**, type the number of minutes in **Web session time-out**.
To disable Web session time-outs, type **0** in the text box.

Disabling Desktop Sharing

The Secure Access Client includes a desktop sharing feature. A user can right-click the Secure Access Client icon in the Windows notification area and select **Share Desktop**. Selecting this option displays a list of all other users who are logged on to the Firebox SSL VPN Gateway from a Secure Access Client.

In some organizations, this feature may cause privacy concerns because it allows any user who logged on through the Secure Access Client to view a list of all other users who are currently logged on.

If you want to prevent a specific group of users from viewing the list of online users, you can disable the desktop sharing feature for an Firebox SSL VPN Gateway user group.

Disabling desktop sharing for a user group causes the following to occur:

- When a member of the user group right-clicks the Secure Access Client icon in the Windows notification area, the **Share Desktop** option is not on the menu. Users in this group cannot display a list of the other online users from the Secure Access Client icon (or use the desktop sharing feature).
- Members of the user group do not appear in the online lists of other users for whom desktop sharing is enabled.

To disable desktop sharing

1 Click the **Access Policy Manager** tab.

2 In the left pane, right-click a group and click **Properties**.

3 On the **General** tab, under **Application options**, select **Disable desktop sharing**.

4 Click **OK**.

Setting Application Options

Application policies limit the network access further by assigning individual network resources to specific applications. Application policies define the network path and endpoint policies for a specific application. When an application policy is created and then added to a user group, the application can use only the specified network path and endpoint policy. This does not prevent other applications from using these resources. To prevent applications from using these network resources, you can deny access to the network.

To deny applications without policies

1 On the **Access Policy Manager** tab, right-click a user group and click **Properties**.

2 On the **General** tab, under **Application Options**, select **Deny applications without policies**.

For more information about application policies, see "Application policies" on page 101.
For more information about endpoint policies, see "End point resources and policies" on page 104.

Enabling Split DNS

By default, the Firebox SSL VPN Gateway checks a user's remote DNS only. You can allow failover to a user's local DNS by enabling split DNS. A user can override this setting using the **Connection Properties** dialog box from the Secure Access logon screen.

To allow failover to a user's local DNS

1 Click the **Access Policy Manager** tab.
2 In the left pane, right-click a group and click **Properties**.
3 On the **Networking** tab, click **Enable split-DNS**.
The Firebox SSL VPN Gateway fails over to the local DNS only if the specified DNS servers cannot be contacted but not if there is a negative response.
4 Click **OK**.

Enabling IP Pooling

In some situations, users connecting using Secure Access Client need a unique IP address for the Firebox SSL VPN Gateway. For example, in a Samba environment, each user connecting to a mapped network drive needs to appear to originate from a different IP address. When you enable IP pooling for a group, the Firebox SSL VPN Gateway can assign a unique IP address alias to each client's session.

You can specify the gateway device to be used for IP pooling. The gateway device can be the Firebox SSL VPN Gateway itself or some other device. If you do not specify a gateway, an Firebox SSL VPN Gateway interface is used, based on the General Networking settings, as follows:

- If you configured only Interface 0 (the Firebox SSL VPN Gateway is inside your firewall), the Interface 0 IP address is used as the gateway.
- If you configured Interfaces 0 and 1 (the Firebox SSL VPN Gateway is in the DMZ), the Interface 1 IP address is used as the gateway. (Interface 1 is considered the internal interface in this scenario.)

To configure IP pooling for a group

1 Click the **Access Policy Manager** tab.
2 In the left pane, right-click a user group and click **Properties**
3 On the **Networking** tab, click **Enable IP pools**.
4 Under **IP Pool Configuration**, right-click a gateway and then click **Modify Gateway Pool**.
5 In **Starting IP Address,** type the starting IP address for the pool.
6 In **Number of IP Addresses**, type the number of IP address aliases. You can have as many as 2000 IP addresses total in all IP pools.
7 In **Default Gateway**, type the gateway IP address.
If you leave this field blank, an Firebox SSL VPN Gateway network adapter is used, as described earlier in this section. If you specify some other device as the gateway, the Firebox SSL VPN Gateway adds an entry for that route in the Firebox SSL VPN Gateway routing table.
8 Click **OK**.

Choosing a portal page for a group

By default, all users log on to the Firebox SSL VPN Gateway using the Secure Access Client from the default portal page or by downloading and installing the Secure Access Client on their computer. You can load custom portal pages on the Firebox SSL VPN Gateway, as described in "Using Portal Pages" on page 38, and then select a portal page for each group. This enables you to control which of the Firebox SSL VPN Gateway clients are available by group.

Note

Disabling portal page authentication on the Global Policies page overrides the Portal Page setting for all groups. For more information, see "Enabling Portal Page Authentication" on page 41.

To specify a portal page for a group

1 On the **Access Policy Manager** tab, under **User Groups**, right-click a group and click **Properties**.

2 On the **Gateway Portal** tab, under **Portal Configuration**, click **Use Custom Portal Page**.

3 In **Use this custom portal page**, select the page.

4 Click **OK**.

Client certificate criteria configuration

To specify criteria that client certificates must meet, use a Boolean expression. To belong to a group, the user must meet the certificate criteria in addition to passing all other authentication rules that are configured for that group. For example, the following criteria requires that the subject field of the client certificate provided by a user has the Organization Unit (OU) set to Accounting and the Common Name (CN) attribute set to a value matching the user's local user name on the Firebox SSL VPN Gateway.

client_cert_end_user_subject_organizational_unit="Accouting" and username=client_cert_end_user_subject_common_name.

Valid operators for the client certificate are as follows:

and logical AND

= equality test

Valid constants for the criteria are:

true logical TRUE

Valid variables for the criteria are:

username local user name on the Firebox SSL VPN Gateway
client_cert_end_user_subject_common_name CN attribute of the Subject of the client certificate
client_cert_end_user_subject_organizational_unit OU attribute of the Subject of the client certificate
client_cert_end_user_subject_organization O attribute of the Subject of the client certificate

Values for the client certificate criteria on the **User Groups** tab require quotation marks around them to work. Correct and incorrect examples are:

The Boolean expression
client_cert_end_user_subject_common_name="clients.gateways.watchguard.com"
is valid and it works.

The Boolean expression
client_cert_end_user_subject_common_name=clients.gateways.watchguard.com
is not valid and does not work

Note

Client certificate configuration is not available for the default user group.

To specify client certificate configuration

1 On the **Access Policy Manager** tab, right-click a group that is not the default group.

2 On the **Client Certificates** tab, under **Client Certificate Criteria Expression**, type the certificate information.

3 Click **OK**.

Global policies

Users can be restricted from logging on to the Firebox SSL VPN Gateway using Global Policies. When users utilize a Web browser to connect to the Firebox SSL VPN Gateway, before they receive the logon dialog box, the end point policy scans the client computer. If the scan fails, users are prevented from logging on. To log on to the Web portal, the client needs to install the correct applications.

To create pre-authentication policies

1 Click the **Access Policy Manager** tab.

2 If an end point policy was created and configured, under **End Point Policies**, click the configured policy and drag it to **Pre-Authentication Policies** in the left pane.

Note

To create and configure end point resources and policies, see "End point resources and policies" on page 104.

Configuring Resources for a User Group

Note

For background information about network access, see "Controlling Network Access" on page 56. Inform users about which resources they can access. A sample email with instructions that you can customize is available from the Administration Portal Downloads page. After making the appropriate changes, send the email to your users.

Resources for user groups are configured on the **Access Policy Manager** tab. The resources include:

- Network Resources
- Application Policies
- File Share Resources
- Kiosk Resources
- End Point Resources
- End Point Policies
- Pre-Authentication Policies

Resources are configured in the right pane of the **Access Policy Manager** tab. When the settings are complete, the resource is dragged to the group in the left pane. For example, you configured and saved

a network resource specifying the networks to which users can connect. If you have a restricted group for contractors, drag the resource to this group and then deny the default setting.

For each user group, you can create an access control list (ACL) by specifying the resources that are to be allowed or denied for the group. Resource groups are defined as described in "Defining network resources" on page 99. ACLs for all groups that users are a part of are combined and applied to the user.

Unless you want to provide all users with full access to all accessible networks, you must associate user groups with resource groups.

Several aspects of Firebox SSL VPN Gateway operation are configured at the group level. These are separated between group properties and group resources.

Group properties include:

- Groups that inherit properties from the Default group.
- Requiring users to log on again if there is a network interruption or if the computer is coming out of standby or hibernate.
- Enabling single sign-on to Windows.
- Enabling single sign-on to the Web Interface.
- Running logon scripts when a user logs on using domain credentials.
- Denying application access to the network that does not have a defined application policy.
- Disable the desktop sharing feature of the Secure Access Client.
- Access configuration to specify the length of time a session is active. There are three types of session time-outs:
  - User session time-out, which specifies the length of time a user can stay logged on, whether there is activity or not. The specified time is absolute. If the user has a 60 minute session time-out, the session ends at 60 minutes. Users are given a one minute warning that their session is about to end.
  - Network activity time-out where the user is logged off after a specified amount of time, during which network activity from the client device over the VPN tunnel is not detected. Network activity from the local area network is not considered.
  - Idle session time-out where network activity is detected, but user activity is not detected. User activities are keyboard strokes or mouse movement.
- Enabling split DNS where the client sends only the traffic destined for the secured network through the VPN tunnel.
- IP pooling where a unique IP address is assigned to each client.
- Logon and portal page usage that defines the page the user sees when logging on. The logon page can be a page provided by WatchGuard and can be modified for individual companies. If your company is using WatchGuard Presentation Server, the logon page can be the Web Interface. If you want to give the user options of how to log on, use the multiple logon option page. For more information, see "Configuring a Portal Page with Multiple Logon Options"

Group resources include:

- Network resources that define the networks to which clients can connect.
- Application policies that define the applications users can use when connected. In addition to selecting the application, you can further define which networks the application has access to and if any end point policies need to be met when connecting.
- File share resources that define which file shares the user can connect to when logged on in kiosk mode.

- Kiosk resources that define how the user can log on and which file shares and applications are accessible to the user when logged on. If the user is allowed to use the Firefox Web browser in kiosk mode, the Web address the user is allowed to use is also defined.
- End point resources and policies that define the required and optional parameters that must be on the user's computer when logging on.

If a user belongs to more than one group, group policies are applied to the user based on the group priorities set on the **Group Priority** tab, as described in "Setting the Priority of Groups".

Adding Users to Multiple Groups

When a user is a member of multiple groups, some group settings are *unioned* together. These settings are:

- Network Resources
- Application Policies
- Kiosk Resources
- End Point Policies

Settings that are not unioned are based on group priority. These include:

- Authenticating after network interruption or on system resume
- Enabling single sign-on
- Running logon scripts
- Session time-out
- Split DNS
- Portal page authentication

Exceptions to the unionized settings are:

- Deny applications without policies. If any of the groups that a user is a member of has the **Deny applications without policies** check box selected, the user inherits that setting.
- IP pooling. Users assume the IP address from the highest priority group that has IP pools enabled.
- Inherit Default group settings. If any of the groups that a user is a part of has the **Inherit properties from the Default Group** check box selected, the user inherits that setting.

Allowing and denying network resources and application policies

By default, all network resources and application policies are allowed. When you deny one resource group, all other resource groups are denied automatically and the network access for the user group is controlled only through its ACL.

The Firebox SSL VPN Gateway interprets allow or deny as follows:

- The Firebox SSL VPN Gateway denies access to any network resource or application policy that is not explicitly allowed. Thus, if you want to provide a particular user group with access to only one resource group, you allow access only to that resource group.
- Deny rules take precedence over allow rules. This enables you to allow access to a range of resources and to also deny access to selected resources within that range. For example, you might want to allow a group access to a resource group that includes 10.20.10.0/24, but need to deny that user group access to 10.20.10.30. To handle this, you create a resource group that includes 10.20.10.30. Access to that resource is denied unless you specifically allow it.

To configure resource access control for a group

1 Click the **Access Policy Manager** tab.

2 In the right pane, configure the group resources.

3 When the resource is configured, click the resource and drag it to the group in the left pane.

4 To allow or deny a resource, in the left pane, right-click the network resource or application policy and then click **Allow** or **Deny**.

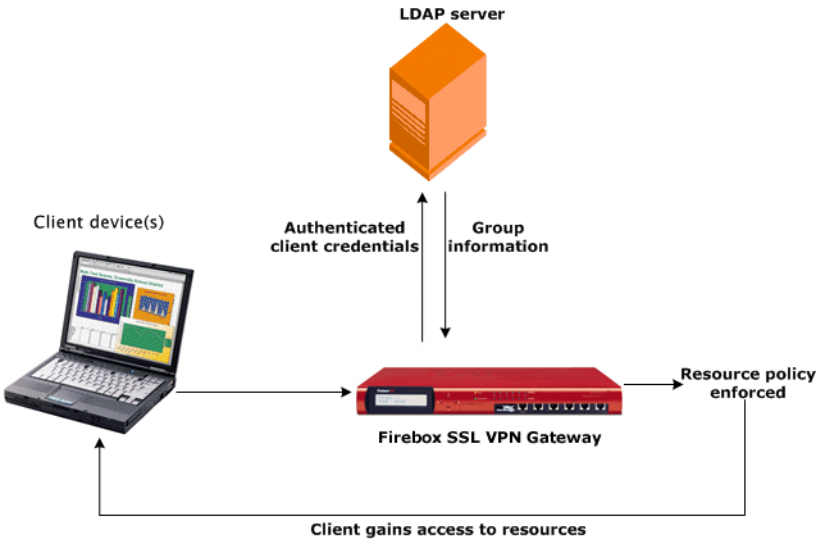
To remove a resource from a user group

1 Click the **Access Policy Manager** tab.

2 In the left pane, right-click the resource you want to remove and then click **Remove**.

Defining network resources

Network resources define the locations that authorized users can access. Resource groups are associated with user groups to form resource access control policies.



Network topology for resource groups and authentication

.

Suppose that you want to provide a user group with secure access to the following:

- The 10.10.x.x subnet
- The 10.20.10.x subnet
- The IP addresses of 10.50.0.60 and 10.60.0.10

To provide that access, create a network resource group by specifying the following IP address/subnet pairs:

```
10.10.0.0/255.255.0.0
10.20.10.0/255.255.255.0
10.50.0.60/255.255.255.255
10.60.0.10/255.255.255.255
```

You can specify the mask in Classless Inter Domain Routing (CIDR) notation. For example, in the above example, you could specify 10.60.0.10/32 for the last entry.

Additional tips for working with resource groups follow.

- You can further restrict access by specifying a port and protocol for an IP address/subnet pair. For example, you might specify that a resource can use only port 80 and the TCP protocol.
- When you configure resource group access for a user group, you can allow or deny access to any resource group. This enables you to exclude a portion of an otherwise allowed resource. For example, you might want to allow a user group access to 10.20.10.0/24 but deny that user group access to 10.20.10.30. Deny rules take precedence over allow rules.
- The easiest method to provide all user groups with access to all network resources is to not create any resource groups and to disable the **Deny Access without ACL** option on the **Global Cluster Policies** tab. All user groups then have access to the accessible networks listed on the **Global Cluster Policies** tab.
- If you have one or more user groups that should have access to all network resources, a shortcut to adding each resource group to those user groups is to create a resource group for 0.0.0.0/0.0.0.0 and allow that one resource group for those user groups. For all other user groups, you will need to allow or deny individual resource groups as needed.

To create and configure a network resource

1 Click the **Access Policy Manager** tab.

2 In the right pane, right-click **Network Resources** and then click **New Network Resource**.

3 Type a name for the group and click **OK**.

4 In **Network/Subnet**, type the IP address/subnet pair for the resource in the Subnets field. You can use CIDR notation for the mask. Use a space to separate entries.

5 In **Port or port range**, enter the port or ports that the Firebox SSL VPN Gateway can use to establish connections with the network resource(s). You have these options when entering ports:
- Enter a 0 (zero) to use all ports.
- Enter a single port or multiple ports that are not in a range. If you enter multiple ports, separate each port with a comma. For example, to allow connections on ports 22, 80, and 8088, enter:
22, 80, 8080
- Enter a range of ports. Separate the starting and ending ports in the range with a hyphen (-). For example, to allow connections on any port from 110 through 120, enter:
110-120
- You can also enter a combination of single ports and a port range. For example, to allow connections on ports 22, 80, 8088 and 110 through 120, enter:
22, 80, 8080, 110-120

6 In **Protocol**, select the protocols that can be used to establish connections on the specified ports.

7 Click **OK**.

Allowing and Denying Network Resources and Application Policies

By default, all network resources and application policies are allowed. When you deny one resource group, all other resource groups are denied automatically and the network access for the user group is controlled only through its ACL.

The Firebox SSL VPN Gateway interprets allow or deny as follows:

- The Firebox SSL VPN Gateway denies access to any network resource or application policy that is not explicitly allowed. Thus, if you want to provide a particular user group with access to only one resource group, you allow access only to that resource group.

- Deny rules take precedence over allow rules. This enables you to allow access to a range of resources and to also deny access to selected resources within that range. For example, you might want to allow a group access to a resource group that includes 10.20.10.0/24, but need to deny that user group access to 10.20.10.30. To handle this, you create two network resources; one that includes the 10.20.10.0/24 subnet and a group that includes 10.20.10.30. Access to that resource is denied unless you specifically allow it.

To add a network resource to a group

1 On the **Access Policy Manager** tab, in the right-pane, under **Network Resources**, click the resource you want to add and then drag it to the user group in the left pane.

2 To allow or deny access, right-click the network resource and then click **Allow** or **Deny**.

To remove a network resource

1 Click the **Access Policy Manager** tab.

2 In the right pane, under **Network Resources**, right-click the resource group you want to remove.

3 Click **Remove**.

Application policies

Application policies put constraints on the network path applications can access. For example, a user is using Microsoft Outlook 2003 for corporate email. You can configure the application to use a specific network resource to the Microsoft Exchange Server. When the network resource is defined, when Outlook tries to start, it checks for the network resource and end point policy (if defined). If it passes, the user can log on and check email. If it fails, Outlook does not start.

If the application is open before connecting to the Firebox SSL VPN Gateway, the application remains open; however, the policies take effect and the user cannot use the application.

If an application policy does not have a network resource or end point policy configured, and if the checkbox **Deny applications without policies** is selected on the **General** tab of the group properties, the application is denied access to the network.

To configure an application policy

1 Click the **Access Policy Manager** tab.

2 In the right pane, right-click **Application Policies** and then click **New Application Policy**.

3 In **Application**, type the name of the application or click **Browse** to navigate to the application.
The MD5 field is populated automatically with the binary sum of the application.

4 To restrict the application to specific networks or require an end point policy, under **Application Constraints** do one or both of the following:
   - To add a network resource to the application policy, under **Network Resources**, click the resource and drag it to **Application Network Policies**.
   - To add an end point policy to the application policy, under **End Point Policies**, click the policy and drag it to **Application End Point Policies**.

5 Click **OK**.

When a user disconnects from the Firebox SSL VPN Gateway, any applications that are open can be closed automatically.

To add an application policy to a group

1 On the **Access Policy Manager** tab, in the right-pane, under **Application Policies**, click the resource you want to add and then drag it to the user group in the left pane.

2 To allow or deny access, right-click the network resource and then click **Allow** or **Deny**.

When an application policy is created and then added to a user group, the application can use only the specified network path and end point policy. This does not prevent other applications from using these resources. To prevent applications from using these network resources, you can deny access to the network.

To deny applications without policies

1 On the **Access Policy Manager** tab, right-click a user group and click **Properties**.

2 On the **General** tab, under **Application options**, select **Deny applications without policies**.

You can deny one application access to the network, while allowing access to all other applications.

A user can get access with this application to all internal networks that were assigned to that user, but the application is denied access to the denied network.

You can also deny all applications access to the network, but allow one to have restricted access to a specific network path. The procedure is the same as "To deny one application network access". The difference is instead of clearing the check box **Deny applications without policies**, it is selected. This check box denies all applications access to the corporate network. To allow one application network access, configure the application policy to accept the application, following the steps in the previous procedure.

Users obtain access to the application only to the internal site that is specifically allowed. No other applications from the client computers are allowed access to the internal network.

To deny one application network access

1 On the **Access Policy Manager** tab, right-click a user group and click **Properties**.

2 On the **General** tab, under **Application Options**, select **Deny applications without policies**.

3 Click **OK** and close the **Properties** dialog box.

4 In the right pane, right-click **Application Policies** and then click **New Application Policy**.

5 Type a name for the policy and click **OK**.

6 Under **Application Resource**, in **Application**, type the application name. When this field is complete, the **MD5** field is populated automatically.

To restrict the application to a specific network path, under Network Resources, click a network resource and drag and drop it on Application Network Policies.

Other configured network resources must already be added to a user group and set to deny. To do so, in the left pane, under **Network Policies** in the group, right-click a network resource and click **Deny**. Click **OK**.

7 Click **OK**.

8 Click the application policy and drag it to the user group to which it applies.

Configuring file share resources

When a user connects from a public computer, the Firebox SSL VPN Gateway opens a kiosk mode connection. The network shares available to the user are configured on the **Access Policy Manager** tab.

To create a file share resource

1 Click the **Access Policy Manager** tab.

2 In the right pane, right-click **File Share Resources**, click **New File Share Resource**, type a name, and click **OK**.

3 In **Share Source,** type the path to the share source using the form: *//server/share*.

4 In **Mount Type,** select the file sharing network protocol, either **CIFS/SMB** or **NFS**.

Note

CIFS/SMB is the Common Internet File System/Server Message Block network protocol used for file sharing in Microsoft Windows. NFS is the Network File System that allows you to mount a disk partition on a remote computer as if it was on the hard drive on the local computer. NFS is typically used with Linux computers.

5 If administrative user credentials are required to mount a CIFS/SMB drive, in **User Name**, specify the user name and in **Password**, type a password. These fields are not enabled for NFS.
All users who access the share have the rights of this user. You might want to create a dummy domain user, like "sslvpn_share" to use for ssl vpn share access.

6 In **Domain,** type the Active Directory domain of the share. This field is not enabled for NFS.

7 In **Permissions**, specify whether you want remote users to have read/write or read-only permissions for the share.

Note

Users can use the FTP protocol to send and receive files to the remote computer.

8 Click **OK**.

To add a share to a group, the share must be added to the kiosk resource first. Then the kiosk resource is dragged and dropped to the group in the left pane.

To remove a share

On the **Access Policy Manager** tab, in the right-pane, right-click the file share and click **Remove**.

Configuring kiosk mode

Kiosk mode is configured using kiosk resources that define the network shares and applications users have access to when they log on in kiosk mode. By default, kiosk mode is disabled. To enable it, the resources are configured and then added to user groups. For more information about client connections, see "Working with Client Connections" on page 117.

Kiosk mode is configured on the **Access Policy Manager** tab and then added to the groups in the left pane.

Note

If the user has general Internet access before making a connection, the user can browse the Internet from the Firefox browser in the Web browser window, unless a network resource is defined that denies access to the Internet.

To create and configure a kiosk resource

1 Click the **Access Policy Manager** tab.

2 In the right pane, right-click **Kiosk Resources** and then click **New Kiosk Resource**.

3 To add a file share, under **File Share Resources**, drag the resource to **Shares** under **File Shares**.

4 Select the applications users are allowed to use in kiosk mode.

5 Click **Kiosk Persistence (Save Application Settings)** to retain Firefox preferences between sessions. The preferences are saved on the remote server (hosting the session).

6 Click **OK**.

7 To add a kiosk resource to a group, click the resource and drag it to the group or groups to which the policy applies.

End point resources and policies

This section describes how to configure end point resources and then create an end point policy.

Configuring end point resources

End point resources provide another layer of security, helping to ensure that users are connecting to the Firebox SSL VPN Gateway on a computer that meets certain criteria. For example, you can require that a computer has particular registry entries, files, and/or active processes. and, optionally, is running one of several specified firewalls.

Each end point rule specifies that a computer must have one, some, or all of the following:

- A registry entry that matches the path, entry type, and value that you specify.
- A file that matches the path, filename, and date that you specify. You can also specify a checksum for the file.
- A running process that you specify. You can also specify a checksum for the file.

End point policies are applied to each group by specifying a Boolean expression that uses end point resource names. For more information, see "Configuring an end point policy for a group" on page 105.

To create an end point resource

1 Click the **Access Policy Manager** tab.

2 In the right pane, right-click **End Point Resources** and then click **New End Point Resource**.

3 Type a name and then click **OK**.

4 In **End point scan type**, select the rule type.

5 Click **Add**.

6 To create a registry rule, do the following:
   - Click **Registry Rule**.
   - In **Registry Path**, type the path and select a key type.
   - In **Registry Entry,** type the key name.
   - In **Registry Value,** type the value to which that key must be set.
   - Click **OK**.

7 To create a **File Rule**, do the following:
   - Click **File Rule**.
   - In **File Name,** type the path and file name or click **Browse** to navigate to the file. The **MD5** field is completed automatically when a file name is entered.
   - In **Date**, type the date in mm/dd/yyyy format.
   - Click **OK**.

8 If you selected **Process Rule**, do the following:
   - Click **Process Rule**.
   - In **Process Name**, type the name of the process or click **Browse** to navigate to the file. The **MD5** field is automatically completed when a process name is entered.

9 Click **OK**.

Note

For information about adding an end point policy to a user group, see "Configuring an end point policy for a group" on page 105.

To delete an end point resource

1 Click the **Access Policy Manager** tab.

2 In the right-pane, right-click the end point resource you want to remove and then click **Remove**.

Configuring an end point policy for a group

The Firebox SSL VPN Gateway Administration Tool allows you to construct an expression by dragging and dropping the end point resource into the End Point Policy Expression Generator. When you drag and drop resources into the generator, the Boolean expression is created automatically for you. Expressions can be modified at any time.

To configure an end point policy for a group, you specify a Boolean expression containing the end point resources that you want to apply to the group.

Suppose that you create the following end point policies:

- CorpAssetRegistryEntry
- AntiVirusProcess1
- AntiVirusProcess2

Your end point policy expression might specify that a registry check must verify that the resource attempting to connect is a corporate asset and that the resource must have one of the antivirus processes running. That Boolean expression is:

```
(CorpAssetRegistryEntry & (AntiVirusProcess1 | AntiVirusProcess2))
```

Valid operators for end point policy expressions are as follows:

( )	- used to nest expressions to control their evaluation
&	- logical AND
|	- logical OR
!	- logical NOT

For users without administrative privileges, end point policies fail if the policy includes a file in a restricted zone (such as C:\Documents and Settings\Administrator) or if the policy includes a restricted registry key.

If a user belongs to more than one group, the end point policy applied to the user is the union of the expression for each of the user's groups.

To create an end point policy for a group

1 Click the **Access Policy Manager** tab.

2 In the right pane, right-click **End Point Policies** and then click **New End Point Policy**.

3 Type a name and click **OK**.

When the policy is created, create the expression by dragging and dropping the end point resources into the **Expression Root**.

To build an end point policy expression

1 Click the **Access Policy Manager** tab.

2 In the right pane, right-click an end point policy and click **Properties**.
The property page opens and the resources pane moves to the left.

3 Under **End Point Scan Expression**, select **Auto-build**.

4 From **End Point Resources**, click and drag a resource to **()Expression Root** in **Expression Generator**.

5 The expression is built using the **AND** identifier. To change the identifier, right-click one of the resources and then select the identifier from the menu.

6 Click **OK**.

The end point policy expression is configured automatically. If you want to manually edit the expression, click to clear **Auto-build**. The **Auto-build** check box should remain selected to prevent errors in the expression.

Setting the Priority of Groups

For users who belong to more than one group, you can determine which group's policies apply to a user by specifying the priority of groups. For example, suppose that some users belong to both the "sales" group and the "support" group. If the sales group appears before the support group in the User Groups list, the sales group policies apply to the users who belong to both of those groups. If the support group appears before the sales group in the list, the support group policies take precedence.

The policies that are affected by the Group Priority setting are as follows:

- Portal page configuration, which determines the portal page the user sees when making a connection. The portal page can be the template provided with the Firebox SSL VPN Gateway or it can point to the Web Interface.
- User time-outs that specify the length of time a session can stay active. Time-outs include:
  - Session time-outs where the connection is closed after a specified amount of time
  - Network activity time-outs where the Secure Access Client does not detect network traffic for a specified amount of time
  - Idle session time-out where the Secure Access Client does not detect mouse or keyboard activity for a specified amount of time
- Enabling split DNS that allows failover to the user's local DNS
- Forcing the user to log on again if there was a network interruption or when the computer comes out of hibernate or standby

The Firebox SSL VPN Gateway looks at all of the user groups. If a user is a member of multiple groups, if the **Deny applications without policies** check box is selected or if **Disable desktop sharing** check box is selected in one group, the user's applications will be denied and desktop sharing will be disabled, regardless of the settings in the other groups.

The following two settings are *unioned* together. For these settings, they are combined among all of the groups of which the user is a member. When these are combined, these are the enforced set of rules applied to the user. For example, if a user is a member of the sales and support groups, if the sales group has notepad.exe and calc.exe defined as an end point policy, and if the support groups have just Internet Explorer defined, all of the policies are enforced for the user.

- Kiosk mode configuration, which includes persistent mode, the applications the user can use, and the default Web address with which the user connects
- End point policies that specify registry settings, processes, or files that must be on the client computer

If users are members of multiple groups, and IP pooling is enabled in one of those groups, the Firebox SSL VPN Gateway allocates an IP address from the pool for the first group that has IP pooling enabled.

Groups are initially listed in the order in which they are created.

To set the priority of groups

1 Click the **Group Priority** tab.

2 Select a group that you want to move and use the arrow keys to raise or lower the group in the list.
The group at the top of the list has the highest priority.

To view the group priorities for a user

In the Firebox SSL VPN Gateway Administration Desktop, click the Real-time Monitor icon.

The display lists all groups to which the user belongs and the group with the highest priority.

Configuring Pre-Authentication Policies

Users can be restricted from logging on to the Firebox SSL VPN Gateway using pre-authentication policies. When users use a Web browser to connect to the Firebox SSL VPN Gateway, before they receive the logon dialog box, the pre-authentication policy scans the client computer. If the scan fails, users are prevented from logging on. To log on to the Web portal, the client needs to install the correct applications.

To create pre-authentication policies

1 Click the **Access Policy Manager** tab.

2 Under **End Point Policies**, click the configured policy and drag it to **Pre-Authentication Policies** in the left pane (located under the **Global Policies** policy node).

To create and configure end point resources and policies, see "Configuring End Point Policies and Resources".

CHAPTER 7

Creating and Installing Secure Certificates

The Firebox SSL VPN Gateway uses certificates for authentication. In the Firebox SSL VPN Gateway Administration Tool, you can create a certificate to be signed by a Certificate Authority. Then, when the signed certificate is received, it can be installed on the Firebox SSL VPN Gateway.

This chapter covers the following topics:

- Generating a Secure Certificate for the Firebox SSL VPN Gateway
- Digital Certificates and Firebox SSL VPN Gateway Operation
- Overview of the Certificate Signing Request
- Client Certificates

Note

When configuring certificates do not use 512-bit keypairs. They are subject to brute force attacks.

Generating a Secure Certificate for the Firebox SSL VPN Gateway

The Firebox SSL VPN Gateway includes a digital certificate that is not signed by a trusted Certificate Authority. Install a digital X.509 certificate that belongs to your company and is signed by a Certificate Authority on the Firebox SSL VPN Gateway. Your company can operate as its own Certificate Authority, or you can obtain a digital certificate from a commercial Certificate Authority such as Verisign and Thawte.

Note

Operating the Firebox SSL VPN Gateway without a digital certificate signed by a Certificate Authority can subject VPN connections to malicious attacks.

There are two ways to install a secure certificate and private key on the Firebox SSL VPN Gateway:

- Generate a Certificate Signing Request using the the Administration Tool. When the request is generated, a certificate and private key are created. The private key remains on the Firebox SSL VPN Gateway and the certificate is sent to a CA for signing. When the certificate is received back, it is installed on the appliance. During installation it is paired with the password-protected private key. WatchGuard recommends using this method to create and install secure certificates.

- Install a PEM certificate and private key from a Windows computer. This methods uploads a signed certificate and private key together. The certificate is signed by a CA and it is paired with the private key.

Digital Certificates and Firebox SSL VPN Gateway Operation

The Firebox SSL VPN Gateway uses digital certificates to encrypt and authenticate traffic over a connection. If the digital certificate installed on the Firebox SSL VPN Gateway is not signed by a Certificate Authority, the traffic is encrypted but not authenticated. A digital certificate must be signed by a Certificate Authority to also authenticate the traffic.

When traffic over a connection is not authenticated, the connection can be compromised through a "man in the middle" attack. In such an attack, a third party intercepts the public key sent by the Firebox SSL VPN Gateway to the Secure Access Client and uses it to impersonate the Firebox SSL VPN Gateway. As a result, the user unknowingly sends authentication credentials to the attacker, who could then connect to the Firebox SSL VPN Gateway. A certificate that is signed by a Certificate Authority prevents such attacks.

If the certificate installed on the Firebox SSL VPN Gateway is not signed by a Certificate Authority, Secure Access users see a security alert when attempting to log on.

Secure Access users see security warnings unless you install a certificate that is signed by a Certificate Authority on the Firebox SSL VPN Gateway and a corresponding certificate on users' computers. Users can also disable the Security Alert through the **Secure Access Connection Properties** dialog box.

Overview of the Certificate Signing Request

Before you can upload a certificate to the Firebox SSL VPN Gateway, you need to generate a Certificate Signing Request (CSR) and private key. The CSR is created using the Certificate Request Generator included in the Administration Tool. The Certificate Request Generator is a wizard that creates a .csr file. When the file is created, it is emailed to the Certificate Authority for signing. The Certificate Authority signs the certificate and returns it to you at the email address you provided. When it is received, you can install it on the Firebox SSL VPN Gateway.

To provide secure communications using SSL/TLS, a server certificate is required on the Firebox SSL VPN Gateway. The steps required to obtain and install a server certificate on the Firebox SSL VPN Gateway are as follows:

- Generate a CSR (myreq.csr) and private key (private.key) using the Certificate Request Generator as described in "Creating a Certificate Signing Request".
- Email the myreq.csr file to an authorized certificate provider.
- When you receive the signed certificate file from your Certificate Authority, upload the certificate using the Administration Tool. The Administration Tool automatically converts the certificate to the PEM format, which is required by the Access Gateway.

Password-Protected Private Keys

Private keys that are generated with the Certificate Signing Request are stored in an encrypted and password-protected format on the Firebox SSL VPN Gateway. When creating the Certificate Signing Request, you are asked to provide a password for the private key. The password is used to protect the

private key from tampering and it is also required when restoring a saved configuration to the Firebox SSL VPN Gateway. Passwords are used whether the private key is encrypted or unencrypted.

Note

Caution: When you upgrade to Version 6.0 and save the configuration file, it cannot be used on earlier versions of the Firebox SSL VPN Gateway. If you attempt to upload the Version 6.0 configuration file to an earlier version, the Firebox SSL VPN Gateway becomes inoperable.

You can also import a password-protected certificate and private key pairs in the PKCS12 format. This allows encrypted and password-protected private keys and certificates created on the Firebox SSL VPN Gateway to be imported.

Note

Caution: If you save the configuration on Version 4.5 of the Firebox SSL VPN Gateway, do not install it on an earlier version of the appliance. Because the private key is encrypted in Version 4.5, older versions cannot decrypt it and the appliance becomes inoperable.

Creating a Certificate Signing Request

The CSR is generated using the Certificate Request Generator in the Firebox SSL VPN Gateway Administration Tool.

To create a Certificate Signing Request

1 Click the **VPN Gateway Cluster** tab and open the window for the appliance.

2 On the **Certificate Signing Request** tab, type the required information in the fields and then click **Generate Request**.

Note

Note: In the field **VPN Gateway FQDN**, type the same FQDN that is on the **General Networking** tab. In **Password**, type the password for the private key.

3 A .csr file is created. Save the certificate request on the local computer.

4 Email the certificate to your Certificate Authority

The certificate provider returns a signed certificate to you by email. When you receive the signed certificate, install it on the Firebox SSL VPN Gateway.

After you create the certificate request and send it to the Certificate Authority, refrain from performing the following tasks on the Firebox SSL VPN Gateway until you receive the signed certificate back and install it on the appliance:

- Generating another Certificate Signing Request
- Uploading a saved configuration file
- Publishing configuration settings from another appliance in the cluster

Note

Important: When the certificate is generated and sent to the Certificate Authority, do not create another Certificate Signing Request. The Firebox SSL VPN Gateway stores one private key. If the Certificate Signing Request is run again, the private key is overwritten and the signed certificate will not match.

Note

When you save the Firebox SSL VPN Gateway configuration, any certificates that are already installed are included in the backup.

To install a certificate file using the Administration Tool

1 Click the **VPN Gateway Cluster** tab.

2 On the **Administration** tab, next to **Upload a signed Certificate (.crt)**, click **Browse**.
This button is used only when you are installing a signed certificate generated on the **Certificate Signing Request** tab.

3 Locate the file you want to upload and click **Open**.

Note

When the client certificate is uploaded, it is converted automatically to PEM format.
You can also upload the certificate using the Administration Portal.

To upload a certificate using the Administration Portal

1 On the **Administration Portal** main page, click **Maintenance**.

2 Next to **Upload Signed Certificate (.crt),** click **Browse.**

3 Navigate to the certificate and upload the file.

Installing a Certificate and Private Key from a Windows Computer

If you are using a load balancer or you have a signed digital certificate with the private key that is stored on a Windows computer, you can upload this to the Firebox SSL VPN Gateway. If the Firebox SSL VPN Gateway is not behind a load balancer, the certificate must contain the FQDN of the Firebox SSL VPN Gateway. If the Firebox SSL VPN Gateway is behind a load balancer, each appliance must contain the same certificate and private key. For more information, see "Connecting to a Server Load Balancer" on page 28.

To install a certificate and private key from a Windows computer

1 Click the **Firebox SSL VPN Gateway Cluster** tab and open the window for the appliance.

2 Click the **Administration** tab.

3 Next to **Upload a .pem private key and signed certificate**, click **Browse**.

4 Navigate to the certificate and then click **Open**.

When you upload the certificate to the Firebox SSL VPN Gateway, you are asked for a password to encrypt the private key.

Installing Root Certificates on the Firebox SSL VPN Gateway

Root certificates are provided by the CA and are used by SSL clients to validate certificates presented by an SSL server.When an SSL client attempts to connect to an SSL server, the server presents a certificate. The client consults its root certificate store to see if the certificate that the SSL server presented is signed by a CA that the root certificate trusts. If you deploy the Firebox SSL VPN Gateway in any environment where the Firebox SSL VPN Gateway must operate as the client in an SSL handshake (initiate encrypted connections with another server), install a trusted root certificate on the Firebox SSL VPN Gateway.

The root certificate that is installed on the Firebox SSL VPN Gateway has to be in PEM format. On Windows, the file extension .cer is sometimes used to indicate that the root certificate is in PEM format.

If you are validating certificates on internal connections, the Firebox SSL VPN Gateway must have a root certificate installed.

To install a root certificate on the Firebox SSL VPN Gateway

1 On the **Firebox SSL VPN Gateway Cluster** tab, open the window for an appliance.
2 On the **Administration** tab, next to **Manage trusted root certificates**, click **Manage**.
3 On the **Manage** tab, click **Upload Trusted Root Certificate**.
4 Navigate to the file and then click **Open**.

To remove the root certificate, click **Remove Trusted Root Certificate**.

Installing Multiple Root Certificates

Multiple root certificates can be installed on the Firebox SSL VPN Gateway, however they must be in one file. For example, you can create a text file in a plain text editor (such as Notepad) that contains all of the root certificates. Open each root certificate in another plain text editor window and then copy and paste the contents of each certificate below the last line in the new text window. When all of the certificates are copied to the new file, save the text file in PEM format, and then upload the file to the Firebox SSL VPN Gateway.

Creating Root Certificates Using a Command Prompt

You can also create PEM-formatted root certificates using a DOS command prompt. For example, if you have three PEM root certificates, you can use the following command to create one file that contains all three certificates:

type root1.pem root2.pem root3.pem > current-roots.pem

If you want to add additional root certificates to an existing file, use the following command:

type root4.pem root5.pem >> current-roots.pem

When this command is executed, all five root certificates are in the file current-roots.pem. The double greater than symbol (>>) appends the the contents of root4.pem and root5.pem to the existing contents of current-roots.pem.

Resetting the Certificate to the Default Setting

The Firebox SSL VPN Gateway comes with a certificate that is not digitally signed by a Certificate Authority. If you need to reimage the appliance, you can reset the certificate to the default certificate that came with the Firebox SSL VPN Gateway. You can do this by using the serial console and selecting the option to reset the certificate.

To reset the default certificate

1 Connect the serial cable to the 9-pin serial port on the Firebox SSL VPN Gateway and connect the cable to a computer that is capable of running terminal emulation software.
2 On the computer, start a terminal emulation application such as HyperTerminal.

Note

Note: HyperTerminal is not installed automatically on Windows 2000 Server or Windows Server 2003. To install HyperTerminal, use Add/Remove Programs in Control Panel.

3 Set the serial connection to 9600 bits per second, 8 data bits, no parity, 1 stop bit. Hardware flow control is optional.

4 Turn on the Firebox SSL VPN Gateway. The serial console appears on the computer terminal after about three minutes.

5 If using HyperTerminal, press the **Enter** key.

6 To reset the default certificate, type **5** and press **Enter**.

Client Certificates

If you want additional authentication, you can configure the Firebox SSL VPN Gateway to require client certificates for authentication.

The Firebox SSL VPN Gateway can authenticate a client certificate that is stored in either of these locations:

- In the certificate store of the Windows operating system on a client computer. In this case, the client certificate is installed separately in the certificate store using the Microsoft Management Console.
- In a smart card or a hardware token. In this case, the certificate is embedded within the smart card and read from a smart card reader attached to the network.

Note

Note: The Firebox SSL VPN Gateway is configured in the same way regardless of whether the certificates are stored in the Windows operating system or on a smart card. No special

If clients are connecting using kiosk mode or from a Linux computer, client side certificates are not supported. If client certificates are enabled in the Firebox SSL VPN Gateway, Linux Clients and kiosk mode do not work.

If a client certificate is required, it must be provided by the network administrator. The certificate is installed separately into the certificate store using the Microsoft Management Console. When this requirement is enforced, every computer that logs on through the Firebox SSL VPN Gateway must have an SSL client certificate that is in P12 format.

To require client certificates

1 Click the **Global Cluster Policies** tab.

2 Under **Select security Options**, select **Require secure client certificates**.

3 Click **Submit**.

Note

Connections using ICA or session reliability do not support client certificates. When client certificates are enabled, the Firebox SSL VPN Gateway accepts only secure connections from applications that can present the client certificate.

Installing Root Certificates

Support for most trusted root authorities is already built into the Windows operating system and Internet Explorer. Therefore, there is no need to obtain and install root certificates on the client device if you are using these CAs. However, if you decide to use a different CA, you need to obtain and install the root certificates yourself.

Obtaining a Root Certificate from a CertificateAuthority

Root certificates are available from the same Certificate Authorities (CAs) that issue server certificates. Well-known or trusted CAs include Verisign, Baltimore, Entrust, and their respective affiliates.

Certificate authorities tend to assume that you already have the appropriate root certificates (most Web browsers have root certificates built-in). However, if you are using certificates from a CA that is not already included on the client computer, you need to specifically request the root certificate.

Several types of root certificates are available. For example, VeriSign has approximately 12 root certificates that they use for different purposes, so it is important to ensure that you obtain the correct root certificate from the CA.

Installing Root Certificates on a Client Device

Root certificates are installed using the Microsoft Management Console (MMC) in Windows. When installing a root certificate to the MMC, use the Certificate Import wizard. The certificate is installed in the Trusted Root Certification Authorities store for the local computer.

For information about root certificate availability and installation on platforms other than 32-bit Windows, refer to product documentation appropriate for the operating system you are using.

Selecting an Encryption Type for Client Connections

All communications between the Secure Access Client and the Firebox SSL VPN Gateway are encrypted with SSL. The SSL protocol allows two computers to negotiate encryption ciphers to accomplish the symmetric encryption of data over a secure connection.

You can select the specific cipher that the Firebox SSL VPN Gateway uses for the symmetric data encryption on an SSL connection. Selecting a strong cipher reduces the possibility of malicious attack. The security policies of your organization may also require you to select a specific symmetric encryption cipher for secure connections.

You can select RC4, 3DES, or AES encryption ciphers for SSL connections. The default setting is RC4 128-bit. The MD5 or SHA hash algorithm is negotiated between the client and the server.

The Firebox SSL VPN Gateway uses RSA for public key encryption in a secure connection. The encryption ciphers and hash algorithms that you can select for symmetric encryption are listed below:

- RC4 128-bit, MD5/SHA
- 3DES, SHA
- AES 128/256-bit, SHA

To select an encryption type for client connections

1 Click the **Global Cluster Policies** tab.

2 Under **Select security options**, in **Select encryption type for client connections**, select the bulk encryption cipher you want to use for secure connections.

3 Click **Submit**.

Requiring Certificates from Internal Connections

To increase security for connections originating from the Firebox SSL VPN Gateway to your internal network, you can require the Firebox SSL VPN Gateway to validate SSL server certificates. Previous versions of the Firebox SSL VPN Gateway did not validate the SSL server certificate presented by the Web Interface and the Secure Ticket Authority. Validating SSL server certificates is an important security measure as it can help prevent security breaches, such as man-in-the-middle attacks.

The Firebox SSL VPN Gateway requires installing the proper root certificates that are used to sign the server certificates.

To install root certificates,

On the **Cluster Config** tab, select **Administration > Manage Trusted root CA certificates**

To require server certificates for internal client connections

On the **Global Cluster Policies** tab, under **SSL Options**, select **Validate SSL Certificates for Internal Connections**.

Wildcard Certificates

The Firebox SSL VPN Gateway supports validation of wildcard certificates for Secure Access Clients. The wildcard certificate has an asterisk (*) in the certificate name. Wildcard certificates can be formatted in one of two ways, such as **.mycompany.com or www*.mycompany.com*. When a wildcard certificate is used, clients can choose different Web addresses, such as http://www1.mycompany.com or http://www2.mycompany.com. The use of a wildcard certificate allows several Web sites to be covered by a single certificate.

CHAPTER 8

Working with Client Connections

Clients can access resources on the corporate network by connecting through the Firebox SSL VPN Gateway from their own computer or from a public computer. The following topics describe how client connections work:

- Using the Access Portal
- Connecting from a Private Computer
- Connecting from a Public Computer
- Client Applications
- Supporting Secure Access Client
- Managing Client Connections

System Requirements

The Secure Access Client is supported on the following operating systems and Web browsers.

Operating Systems

The Secure Access Client is supported on the following Windows operating systems:

- Windows XP Home Edition
- Windows XP Professional
- Windows 2000 Server
- Windows Server 2003
- Windows Vista 32-bit

Web Browsers

The Secure Access Client is supported on the following Web browsers:

- Microsoft Internet Explorer, Versions 6.*x* and 7.*x*
- Mozilla Firefox Version 1.5 and later versions

If clients are using Mozilla Firefox to connect, pages that require ActiveX, such as the pre-authentication page, are not able to run.

If clients are going to connect using the kiosk, they must have Sun Java Runtime Environment (JRE) Version 1.5.0_06 installed on their computer.

Using the Access Portal

The Access Portal is an HTML page that enables a user to choose the type of connection to be established from a remote computer. Users can either connect from the portal page or they can use the Secure Access Client that is installed on their computer from the portal page.

Note

You can customize the portal page templates provided with the Firebox SSL VPN Gateway and assign them on a group basis, as described in "Using Portal Pages" on page 38 and "Client certificate criteria configuration" on page 95. You can also include a link to the Firebox SSL VPN Gateway Clients on a Web site, as described in "Linking to Clients from Your Web Site" on page 41.

From the portal page, the user either starts the Secure Access Client or kiosk mode.

- The Secure Access Client is intended for connections from a private computer because data is transferred from the network to which the user is connecting to the user's computer.
- Kiosk mode is useful for connections from a public computer because no data is written to the user's computer. However, if you configure network shares, a user can copy files from a shared network drive to the remote computer.

Note

You can configure the Firebox SSL VPN Gateway Administration Tool so that users do not have the option to connect from a public computer. For more information, see "End point resources and policies" on page 104

To connect using the default portal page

1. Use Internet Explorer to access the Web address of the Firebox SSL VPN Gateway; for example: https://vpn.mycompany.com.
2. If the Firebox SSL VPN Gateway does not have a signed certificate installed, a Security Alert dialog box appears. Click **Yes** to continue.
3. Type the network user name and password and then click **Connect**.
   The default portal page opens.
4. If connecting from a Windows computer, choose the type of connection:
   - If connecting from a secure computer, click **My own computer**.

   The first time a connection is made, the **File Download** dialog box appears. Click **Save** and then click **Open**. The file downloads to the client computer. The first time that you connect to the Firebox SSL VPN Gateway, the **Terms and Conditions of Use** dialog box appears. You must click "I Accept" to install the driver. When the driver is installed, the user can subsequently start the Secure Access Client without going through the portal page.

   If you configured the Secure Access Client to start automatically, the client starts after the users enter their Windows logon credentials, which are also used for the Secure Access Client. Thus, when

the computer is started, users do not have to do anything to create the connection, provided that they have a network connection and can log onto Windows.

The connection enables users to work with the connected site just as if they were logged on at the site. Data can be transferred between the remote computer and the connected site. For more information, see "Connecting from a Private Computer" on page 119.

If connecting from a public computer, click **A public computer**.

The Web browser opens in one of two configured modes, as described in "Connecting from a Public Computer" on page 126.

5 If connecting from a Linux computer, click the Linux download link to start the download and view instructions about how to install the client.

Note

The Linux tcl and tk packages are required for the Secure Access Client..

In addition to the command net6vpn --login, which opens the logon dialog box for the Secure Access Client, you can also type **net6vpn** to see a list of other command-line options. If you lose the connection, the VPN daemon may be stopped. The Secure Access Client requires a running VPN daemon to connect to the Firebox SSL VPN Gateway. To check the status of the VPN daemon, type the following at a command prompt:

/sbin/service net6vpnd status

To restart a stopped daemon, type the following:

/sbin/service net6vpnd start

Then, click **Disconnect** and reenter your logon credentials.

To remove the Linux VPN client

At the command prompt, type the following:

/sbin/service net6vpnd stop
/sbin/chkconfig --del net6vpnd
rm -rf /etc/net6vpn.conf /etc/init.d/net6vpnd /usr/bin/net6vpn /usr/sbin/net6vpnd /usr/local/net6vpn/

Connecting from a Private Computer

If a user chooses the **My own computer** option in the Access Portal page, the connection provides full access to the network resources that the user's group(s) have permission to access.

The Firebox SSL VPN Gateway operates as follows:

- When a user firsts connects using a Web address, the Secure Access Client is downloaded and installed onto the client computer.
- After downloading the Secure Access Client, the user logs on. When the user successfully authenticates, the Firebox SSL VPN Gateway establishes a secure tunnel.
- As the remote user attempts to access network resources across the VPN tunnel, the Secure Access Client encrypts all network traffic destined for the organization's intranet and forwards the packets to the Firebox SSL VPN Gateway.

- The Firebox SSL VPN Gateway terminates the SSL tunnel, accepts any incoming traffic destined for the private network, and forwards the traffic to the private network. The Firebox SSL VPN Gateway sends traffic back to the remote computer over a secure tunnel.

When a remote user logs on using the Secure Access Client, the Firebox SSL VPN Gateway prompts the user for authentication over HTTP 401 Basic or Digest. The Firebox SSL VPN Gateway authenticates the credentials using an authentication type such as local authentication, RSA SecurID, SafeWord, LDAP, NTLM, or RADIUS. If the credentials are correct, the Firebox SSL VPN Gateway finishes the handshake with the client. This logon step is required only when a user initially downloads the Secure Access Client.

If the user is behind a proxy server, the user can specify the proxy server and authentication credentials. For more information, see "Configuring Proxy Servers for the Secure Access Client" on page 125.

The Secure Access Client is installed on the user's computer. After the first connection, the remote user can subsequently use a desktop shortcut to start the Secure Access Client.

The **Advanced Options** dialog box, which is used to configure client computer settings, can also be opened by right-clicking the Secure Access Client icon on the desktop and then clicking **Properties**.

If users are connecting using a Web page, they are either prompted to log on or are taken directly to a portal page where they can connect using Secure Access Client.

If the Firebox SSL VPN Gateway is configured to have users log on before making a connection with Secure Access Client, they type their user name and password and then log on. A portal page appears that provides the choice to log on using the full Secure Access Client or in kiosk mode (if enabled). If a user chooses to log on using Secure Access Client, the connection provides full access to the network resources that the user's group(s) have permission to access.

The access granted by the security policies enable users to work with the remote system just as if they are logged on locally. For example, users might be granted permission to applications, including Web, client-server, and peer-to-peer such as Instant Messaging, video conferencing, and real-time Voice over IP applications. Users can also map network drives to access allowed network resources, including shared folders and printers.

While connected to an Firebox SSL VPN Gateway, remote users cannot see network information from the site to which they are connected. For example, while connected to the Firebox SSL VPN Gateway, type the following at a command prompt:

```
ipconfig/all or route print
```

You will not see network information from the corporate network.

Establishing the Secure Tunnel

After the Secure Access Client is started, it establishes a secure tunnel over port 443 (or any configured port on the Firebox SSL VPN Gateway) and sends authentication information. When the tunnel is established, the Firebox SSL VPN Gateway sends configuration information to the Secure Access Client describing the networks to be secured and containing an IP address if you enabled IP pooling. For more information about IP pooling see "Enabling IP Pooling" on page 94.

Tunneling Private Network Traffic over Secure Connections

When the Secure Access Client is started and the user is authenticated, all network traffic destined for specified private networks is captured and redirected over the secure tunnel to the Firebox SSL VPN Gateway.

The Firebox SSL VPN Gateway intercepts all network connections made by the client device and multiplexes/tunnels them over SSL to the Firebox SSL VPN Gateway, where the traffic is demultiplexed and the connections are forwarded to the correct host and port combination.

The connections are subject to administrative security policies that apply to a single application, a subset of applications, or an entire intranet. You specify the resources (ranges of IP address/subnet pairs)

that remote users can access through the VPN connection. For more information, see "Configuring Resources for a User Group" on page 96.

All IP packets, regardless of protocol, are intercepted and transmitted over the secure link. Connections from local applications on the client computer are securely tunneled to the Firebox SSL VPN Gateway, which reestablishes the connections to the target server. Target servers view connections as originating from the local Firebox SSL VPN Gateway on the private network, thus hiding the client IP address. This is also called *reverse Network Address Translation* (NAT). Hiding IP addresses adds security to source locations.

Locally, on the client computer, all connection-related traffic (such as SYN-ACK, PUSH, ACK, and FIN packets) is recreated by the Secure Access Client to appear from the private server.

Operation through Firewalls and Proxies

Users of Secure Access Client are sometimes located inside another organization's firewall. NAT firewalls maintain a table that allows them to route secure packets from the Firebox SSL VPN Gateway back to the client computer. For circuit-oriented connections, the Firebox SSL VPN Gateway maintains a port-mapped, reverse NAT translation table. The reverse NAT translation table enables the Firebox SSL VPN Gateway to match connections and send packets back over the tunnel to the client with the correct port numbers so that the packets return to the correct application.

The Firebox SSL VPN Gateway tunnel is established using industry-standard connection establishment techniques such as HTTPS, Proxy HTTPS, and SOCKS. This operation makes the Firebox SSL VPN Gateway firewall accessible and allows remote computers to access private networks from behind other organizations' firewalls without creating any problems.

For example, the connection can be made through an intermediate proxy, such as an HTTP proxy, by issuing a CONNECT HTTPS command to the intermediate proxy. Any credentials requested by the intermediate proxy are in turn obtained from the remote user (by using single sign-on information or by requesting the information from the remote user) and presented to the intermediate proxy server. When the HTTPS session is established, the payload of the session is encrypted and carries secure packets to the Firebox SSL VPN Gateway.

Terminating the Secure Tunnel and Returning Packets to the Client

The Firebox SSL VPN Gateway terminates the SSL tunnel and accepts any incoming packets destined for the private network. If the packets meet the authorization and access control criteria, the Firebox SSL VPN Gateway regenerates the packet IP headers so that they appear to originate from the Firebox SSL VPN Gateway's private network IP address range or the client-assigned private IP address. The Firebox SSL VPN Gateway then transmits the packets to the network.

Note

Note: The Secure Access Client maintains two tunnels: an SSL tunnel over which data is sent to the Firebox SSL VPN Gateway and a tunnel between the client and local applications. The encrypted data that arrives over the SSL tunnel is then decrypted before being sent to the local application over the second tunnel.

If you run a packet sniffer such as Ethereal on the computer where the Secure Access Client is running, you will see unencrypted traffic that appears to be between the client and the Firebox SSL VPN Gateway. That unencrypted traffic, however, is not over the tunnel between the client and the Firebox SSL VPN Gateway but rather the tunnel to the local applications.

When an application client connects to its application server, certain protocols may require that the application server in turn attempt to create a new connection with the client. In this case, the client

sends its known local IP address to the server by means of a custom client-server protocol. For these applications, the Secure Access Client provides the local client application a private IP address representation, which the Firebox SSL VPN Gateway uses on the internal network. Many real-time voice applications and FTP use this feature.

Clients can access resources on the corporate network by connecting through the Firebox SSL VPN Gateway from their own computer or from a public computer.

ActiveX Helper

When the user connects to the Web Interface portion of the Firebox SSL VPN Gateway and logs on, net6helper.cab and ActiveX control are installed. This file provides three main functions:

- It launches the client from the Web page instead of having to manually download the executable and then launching the Secure Access Client.
- It performs pre-authentication checks for the Web page.
- It provides single sign-on. When the Secure Access Client is started from the Web page, the Secure Access Client does not prompt the user to log on again.

Using the Secure Access Client Window

To enable users to connect to and use the Firebox SSL VPN Gateway, you need to provide them with the following information:

- Firebox SSL VPN Gateway Web address, such as https://*AccessGatewayFQDN*/.

If a user needs access from a computer that is not running Windows 2000 or above or Linux, but is running a Java Virtual Machine (JVM) 1.5 or higher, the user can use the Java applet version of the kiosk. The Web address for connecting to the Java applet version of the kiosk is: https://AccessGateway/vpn_portal-javaonly.html

- The authentication realm name required for logon (if you use realms other than the realm named Default).
- Path to any network drives that the users can access, which is done by mapping a network drive on their computer.
- Any system requirements for running the Secure Access Client if you configured end point resources and policies.

Depending on the configuration of a remote user's system, you might also need to provide additional information:

- To start the Secure Access Client**,** Windows 2000 users must be a local administrator or a member of the Administrators group to install programs on their computer. This restriction applies to Windows XP for first-time installation only, not for upgrades.
- If a user runs a firewall on the remote computer, the user might need to change the firewall settings so that it does not block traffic to or from the IP addresses corresponding to the resources for which you granted access. The Secure Access Client automatically handles Internet Connection Firewall in Windows XP and Windows Firewall in Windows XP Service Pack 2. For information about configuring a variety of popular firewalls, see "Using Firewalls with Firebox SSL VPN Gateway" on page 149.
- Users who want to send traffic to FTP over the Firebox SSL VPN Gateway connection must set their FTP application to perform passive transfers. A passive transfer means that the remote computer establishes the data connection to your FTP server, rather than your FTP server establishing the data connection to the remote computer.
- Users who want to run X client applications across the connection must run an X server, such as XManager, on their computers.
- Because users work with files and applications just as if they were local to the organization's network, no retraining of users or configuration of applications is needed.

An email template is provided that includes the information discussed in this section. The template is available from the Downloads page of the Administration Portal. WatchGuard recommends that you customize the text for your site and then send the text in an email to users.

When the Secure Access Client is loaded, users are prompted to log on to the Firebox SSL VPN Gateway to establish the connection. The Firebox SSL VPN Gateway administrator determines the type of authentication using the **Authentication** tab of the Firebox SSL VPN Gateway Administration Tool, as described in "Configuring Authentication and Authorization" on page 61.

If double-source authentication is configured on the Firebox SSL VPN Gateway, and the users are logging on using full access, they type their user name and passwords for each type of authentication. For example, users are configured to use LDAP authentication and RSA SecurID. They would type their password, their RSA SecurID personal identification number (PIN), and RSA SecureID code. For more information about logging on using double-source authentication, see "Double-source Authentication Portal Page" on page 43.

Note

If you are using the Linux Client, the connection window will not include the options described in the following procedure.

The Secure Access Client is installed the first time the user logs on to the portal Web page.

To log on to the Firebox SSL VPN Gateway

1 In the **Firebox SSL Secure Access** dialog box, enter the logon credentials.

If the Firebox SSL VPN Gateway is configured with more than one authentication realm and you need to connect to a realm other than the Default, enter the realm name before your user name (*realmName\userName)*.

If your site uses RSA SecurID authentication, your password is your PIN plus the RSA SecurID token.

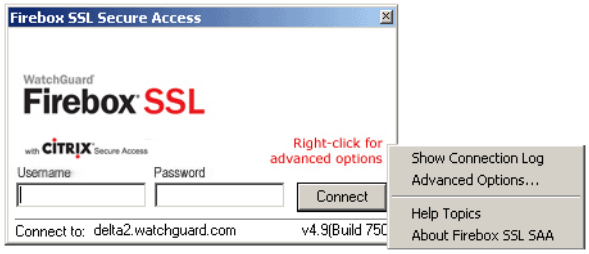
2 If the Firebox SSL VPN Gateway requires double-source authentication, type the user name and the password for each authentication type.

The Secure Access Client dialog box showing double-source authentication

Note

When a user logs on, the authentication is checked in the order that is configured in the realm. If the user log on fails the primary authentication, the secondary authentication is not checked.

3 If you are behind a proxy server, right-click the dialog box and then click **Advanced Options**.



The Secure Access Client dialog box with the pop-up menu showing Advanced Options

4 Under **Proxy Settings,** select **Use Proxy Host** and then in **Proxy Address** and **Proxy Host,** type the IP address and port. If the proxy server requires authentication, select **Proxy server requires authentication**. When users attempt to establish a connection, they are first prompted for their proxy server logon credentials.

5 To allow failover to your local DNS, under **Connection Settings**, select **Enable Split DNS**.

6 To allow the Secure Access Client to update automatically, without prompts, when a new version is available on the Firebox SSL VPN Gateway, under **Connection Settings**, select the **Always update client** check box.

7 Click **OK** and then click **Connect**.

Note

If a digital certificate signed by a Certificate Authority is not installed on the Firebox SSL VPN Gateway, you will see a Security Alert. For more information, see "Digital Certificates and Firebox SSL VPN Gateway Operation" on page 110.

When the connection is established, a status window briefly appears and the Secure Access Client window is minimized to the notification area. The icon indicates whether the connection is enabled or disabled and flashes during activity.

A shortcut to the Secure Access Client is placed on the desktop.

To use the Secure Access Client status properties

1 To open the window, double-click the connection icon in the notification area. Alternatively, right-click the icon and choose **VPN Properties** from the menu.
The Secure Access Client dialog box appears.

2 To view the properties of the connection, click the **General**, **Details** or **Access Lists** tabs. These tabs provide information that is helpful for troubleshooting. The properties include:
- The **General** tab displays connection information.
- The **Details** tab displays server information and a list of the secured networks the clients are allowed to access.
- The **Access Lists** tab displays the access control lists (ACLs) that are configured for the user connection. This tab does not appear for users who are not in a group or if an ACL is not configured for a group.

3 To close the window, click **Close**.

To disconnect the Secure Access Client

Right-click the Secure Access icon in the notification area and choose **Disconnect** from the menu.

To view the Connection Log

The Connection Log contains real-time connection information that is particularly useful for trouble-shooting connection issues.

1 Right-click the Firebox SSL Secure Access Client icon in the notification area.

2 Choose **Connection Log** from the menu.
The Connection Log for the session appears.

Note

The Connection Log is written to the computer in %systemroot\Documents and Settings\username\Local Settings\Application Data\NET6\net6vpn.log. The log is overwritten each time a new VPN connection is established.

To disconnect the Secure Access Client

Right-click the Secure Access Client icon in the notification area and choose **Disconnect** from the menu.

Note

When you share an application, instead of your desktop, the person with whom you are sharing the application can view and work with only that application. The rest of your desktop is not visible to the other person.

Configuring Proxy Servers for the Secure Access Client

When the Secure Access Client connects, before downloading polices from the Firebox SSL VPN Gateway, the Secure Access Client queries the operating system for client proxy settings. If auto-detection is enabled, the Secure Access Client automatically changes client proxy settings to match settings stored in the operating system. The Secure Access Client attempts to connect to the Firebox SSL VPN Gateway, download pre-authentication policies, and then prompt the users for their logon credentials. If the Secure Access Client cannot automatically detect the client proxy settings, it resorts to a straight connection without using the proxy server. Automatic detection of the proxy settings is configured in the **Advanced Options** dialog box in the Secure Access Client.

Users can also manually configure a proxy server from the Secure Access Client. When a proxy server is manually configured, this disables the automatic detection of proxy settings.

To manually configure a proxy server

1 On the desktop of the client computer, click the Secure Access Client icon to open the logon dialog box.

2 Right-click anywhere in the **Secure Access Client** logon dialog box and select **Advanced Options**.

3 In the **WatchGuard Secure Access Options** dialog box, under **Proxy settings**, select **Manually configure proxy server**.

4 In **IP Address** and **Port**, type the IP address and port number.

5 If authentication is required by the server, select **Proxy server requires authentication**.

The **Advanced Options** dialog box can also be opened by right-clicking the WatchGuard Secure Access icon on the desktop and then clicking **Properties**.

Configuring Secure Access Client to Work with Non-Administrative Users

If a user is not logged on as an administrator on a computer running Windows 2000 Professional, the Secure Access Client must be installed locally on the client computer and then started using the Web address of https://*FQDN*/ WatchGuardsaclient.exe, where *FQDN* is the address of the Firebox SSL VPN Gateway. The ActiveX applet does not have the rights to download and install the file. Clients who are logged on as non-administrators using Windows 2003 Server or Windows XP are able to download and install the ActiveX applet.

For a user who is not logged on as an administrator and connects using the Secure Access Client, applications such as Microsoft Outlook might occasionally lose the network connection.

Connecting from a Public Computer

Connections Using Kiosk Mode

The Firebox SSL VPN Gateway provides secure access to a corporate network from a public computer using kiosk mode. When users select **A public computer** on the WatchGuard portal page, a Web browser opens. The user logs on and then can access applications provided in the browser window.

By default, kiosk mode is disabled. When kiosk mode is disabled, users do not see the **A public computer** option on the portal page and the Firebox SSL VPN Gateway does not provide any kiosk mode functionality.

For computers running Java virtual machine (JVM 1.5) or higher (such as Macintosh, Windows 95, or Windows 98 computers), kiosk mode is available through a Java applet. For Macintosh computers to support kiosk mode, the Safari browser and JRE 1.5 must be installed.

When the user is logged on using kiosk mode, the Firebox SSL VPN Gateway sends images only (no data) over the connection. As a result, there is no risk of leaving temporary files or cookies on the public computer. Both temporary files and cookies for the session are maintained on the Firebox SSL VPN Gateway.

The browser defaults to a Web address that is configured per group through the Administration Tool. The Web browser window can also include icons for Remote Desktop, SSH, Telnet 3270 emulator, Gaim instant messenging, and VNC clients. The icons are displayed in the bottom-left corner of the window. The applications are specified for each group. For more information about configuring applications for kiosk mode, see "Creating a Kiosk Mode Resource" on page 127.

The Web browser window also provides access to shared network drives. The Firebox SSL VPN Gateway administrator configures the permissions granted (read-only or read/write) to each shared network drive. For more information about configuring network shares, see "Configuring file share resources" on page 102.

Users can copy files from the network share to their computer simply by dragging the file onto the KioskFTP icon and selecting the destination in the **File Download** dialog box.

Note

Important: End point policies are not supported or enforced when users are logged on using kiosk mode.

Kiosk mode can include the following applications if they are enabled on the **User Groups** tab in the Administration Tool:

- Firefox Web browser. You configure by group whether or not to include the Firefox browser and the browser's default Web address. Firefox preferences, such as saved passwords, are retained for the next session.
- Shared network drives. Icons that provide access to shared network drives. The user can download files from a network share by dragging a file onto the KioskFTP icon, as described in "Configuring File Shares for Kiosk Mode" on page 141.
- Icons that provide access to the VNC client, Remote Desktop, Telnet 3270 emulator, and SSH. You configure by group the clients to be included in the kiosk session.

For information about using the clients, see the following sections:

- "Remote Desktop client" on page 130
- "SSH Client" on page 130
- "Telnet 3270 Emulator Client" on page 131
- "VNC Client" on page 131
- "Gaim Instant Messenging" on page 131

If the user's browser is configured to use a proxy server, users connected using kiosk mode use the browser's proxy setting.

To allow users access to corporate resources using kiosk mode, it must be enabled.

To enable kiosk mode

On the **Global Cluster Policies** tab, under **Access options**, select **Enable kiosk mode**.

If this check box is clear, users cannot use kiosk mode and the option is not available from the Web portal page.
When kiosk mode is enabled, users can connect using the Web portal page.

To log on to the Firebox SSL VPN Gateway using kiosk mode

1 Use the logon page to connect, as described in "Connecting Using a Web Address". Click **A public computer**.
The WatchGuard Secure Access logon dialog box appears.
2 Enter your network logon credentials and click **Login**.

Note

Note: Users logged on using kiosk mode can use the FTP protocol to download files from the corporate network. Files that are downloaded using the kiosk session cannot be returned to the corporate network.

Creating a Kiosk Mode Resource

Kiosk mode is configured using kiosk resources that define the file shares and applications users have access to when they log on in kiosk mode. By default, kiosk mode is disabled. To enable it, the resources are configured and then added to user groups.

Kiosk mode is configured on the **Access Policy Manager** tab and then added to the groups in the left pane.

Note

Note: If the user has general Internet access before making a connection, the user can browse the Internet from the Firefox browser in the Web browser window, unless a network resource is defined that denies access to the Internet.

To create and configure a kiosk resource

1 Click the **Access Policy Manager** tab.

2 In the right pane, right-click **Kiosk Resources** and then click **New Kiosk Resource**.

3 Type a name for the resource and click **OK**.

4 To add a file share, under **File shares**, drag the resource to **Shares**.

5 Select the applications users are allowed to use in kiosk mode.

6 Select **Save kiosk application settings** to retain Firefox preferences between sessions. The preferences are saved on the remote server (hosting the session). Click **OK**.

7 To add a kiosk resource to one or more groups, click the resource and drag it to the group or groups to which the policy applies.

Working with File Share Resources

When a user connects with a Web browser and selects **A public computer**, the Firebox SSL VPN Gateway opens a kiosk connection. If file shares are configured, the user can work with files that reside on the share. Files are not downloaded to the public computer. The network shares available to the user are configured on the **Access Policy Manager** tab.

To create a file share resource

1 Click the **Access Policy Manager** tab.

2 In the right pane, right-click **File Share Resources**, click **New File Share Resource**, type a name, and click **OK**

3 In **Share source,** type the path to the share source using the form: *//server/share*.

4 In **Mount type,** select the file sharing network protocol, either **CIFS/SMB** or **NFS**.

Note

Note: CIFS/SMB is the Common Internet File System/Server Message Block network protocol used for file sharing in Microsoft Windows. NFS is the Network File System that allows you to mount a disk partition on a remote computer as if it was on the hard drive on the local computer. NFS is typically used with Linux computers.

5 If administrative user credentials are required to mount a CIFS/SMB drive, in **User name**, specify the user name and in **Password**, type a password. These fields are not enabled for NFS.
All users who access the share have the rights of this user.

6 In **Domain,** type the Active Directory domain of the share. This field is not enabled for NFS.

7 In **Permissions**, specify whether you want remote users to have read/write or read-only permissions for the share. Click **OK.**

Note

Note: Users can use the FTP protocol to send and receive files to the remote computer.

After configuring the file share, it must be added to the kiosk resource.

To add a file share to a kiosk resource

1 On the **Access Policy Manager** tab, in the right-pane, under **Kiosk Resources**, right-click a resource, and click **Properties**.

2 Select a file share from **File Share Resources** and drag it to **Shares** under **File shares** in the kiosk resource.

3 Click **OK.**

To remove a file share

On the **Access Policy Manager** tab, in the right-pane, right-click the file share and click **Remove**.

You can specify the shared network drives that are accessible for sessions. For each shared drive, you specify whether users have read-only or read/write access. If users are granted read-write access, a user can change the files on the shared network drive, provided that the user's account has the permissions to do so.

To work with file share resources

1 In the Web browser, double-click a shared network drive icon.
The share window opens inside of the kiosk window.

2 To copy a file from the network drive to your computer, drag the file icon over the KioskFTP icon.

3 In the **Kiosk File Download** dialog box, navigate to the location where you want to copy the file and then click **Open**.

When the FTP transfer is complete, a message window appears.

You cannot use FTP to transfer folders or copy files back to the shared network drive.

Client Applications

When users are logged on using kiosk mode, you can allow them to use different applications. The applications include:

- Firefox web browser
- Remote Desktop Client
- SSH Client
- Telnet 3270 Emulator Client
- VNC Client
- Gaim Instant Messenging

Configuration of these client applications is done on the **Access Policy Manager** tab in the Administration Tool.

To enable client applications

1 Click the **Access Policy Manager** tab.

2 2. In the right pane, under **Kiosk Resources**, right-click a resource and click **Properties**.

If you are enabling Firefox, type the Web address of the browser.

If you are enabling Remote Desktop, type the IP address of the remote computer.

3 Under **Kiosk Resource**, select the applications users are allowed to use. Click **OK**.

4 Drag the resource to the group or groups to which it belongs.

5 Click **OK**.

Firefox Web Browser

The Firefox Web browser allows users to connect to the Internet when they are logged on in kiosk mode. They can connect to Web sites as if they were sitting at their own computer.

To configure Firefox

1 Click the **Access Policy Manager** tab.

2 In the right pane, under **Kiosk Resources**, right-click a resource and click **Properties**.

3 Select **Enable Firefox** and in the text box, type the Web address for the browser.

Remote Desktop client

The Remote Desktop client enables a user to remotely access the desktop of a server that is running Windows Terminal Services. The Remote Desktop does not require any configuration on the user's computer.

If Remote Desktop is configured for kiosk mode, it is the only application that can be used by the client. When the client connects using kiosk mode and then starts the Remote Desktop connection, the Remote Desktop session takes control of the session. It is not possible to switch back between the kiosk session and Remote Desktop. If other clients, such as VNC or SSH are configured, Remote Desktop cannot be configured.

To configure Remote Desktop

1 On the **Access Policy Manager** tab, right-click **Kiosk Resources**.

2 Type a name for the resource and click **OK**.

3 Select **Remote Desktop** and type the FQDN of the server in the text box. Click **OK**.

Remote Desktop provides the user with full access to a remote computer's resources, including files, applications, and network resources. Thus, the user can remotely control the computer, just as if the user is sitting at it. The user's work remains on the remote computer; no files, only images, are sent to the user's computer.

When users log on from a public computer, and Remote Desktop is configured, there is an icon that they can click to start Remote Desktop. After typing their user name and password, the desktop of the remote computer appears on the public computer.

To use the Remote Desktop client

1 From the portal page, choose **A public computer** and log on.

2 In the Web browser, click the Remote Desktop icon.

3 Enter the user name and the remote host and click **Connect**.

4 In the Windows logon screen, enter the credentials and network name of the remote server.
The desktop of the Remote Desktop server displays in a window on your computer.

5 Work with the remote server just as if it was your local computer.

SSH Client

The SSH client enables the user to establish an SSH connection to a remote computer.

To use the SSH client

1. From the portal page, choose **A public computer** and log on.
2. In the Web browser, click the SSH icon.
3. Enter the user name and SSH host name or IP address.
   The SSH window opens.

Telnet 3270 Emulator Client

The Telnet 3270 Emulator client enables the user to establish a Telnet 3270 connection to a remote computer.

To use the Telnet 3270 Emulator client

1. From the portal page, choose **A public computer** and log on.
2. In the Web browser, click the Telnet 3270 Emulator icon.
   The x3270 window opens.
3. On the **Connect** menu, choose **Other**.
   The x3270 Connect window opens.
4. Enter the host name or IP address and click **Connect** to log on and receive a prompt.
5. To view the 3270 keypad, click the keypad icon in the upper-right corner.

VNC Client

The VNC client enables a user to remotely access the desktop of a VNC server. The user's work remains on the remote server; no files, only images, are sent to the user's computer.

To use the VNC client

1. From the portal page, choose **A public computer** and log on.
2. In the Web browser, click the VNC icon.
3. In **VNC Host,** type the IP address of the VNC host, and in **Password,** type the password for the server and click **Connect**.
   The desktop of the VNC server displays in a window on your computer.
4. Work with the remote server just as if it were your local computer.

Note

To send a Ctrl+Alt+Del to the connected server through the VNC server, press **Shift+Ctrl+Alt+Delete**.

Gaim Instant Messenging

Gaim is an instant messaging client that supports multiple instant messenging applications including:

- AOL Instant Messenger
- ICQ (Oscar Protocol)
- MSN Messenger
- Yahoo! Messenger
- IRC

Gaim users can log on to multiple accounts of different instant messenging networks at the same time.

To use Gaim

1 From the portal page, choose **A public computer** and log on.

2 In the Web browser, double-click the Gaim icon.

3 If messenging services were not added, an **Accounts** window opens. Click **Add**.

4 In the **Add Account** dialog box, in **Protocol**, select the instant messenging service to add.

5 Complete the rest of the information and click **Save**.

6 Repeat, adding instant messenging services for each product.

7 To log on to an instant messenging service, in the Gaim **Login** dialog box, in **Account**, select the service, type the password, and then click **Sign on**.

Supporting Secure Access Client

To enable users to connect to and use the Firebox SSL VPN Gateway, you need to provide them with the following information:

- Firebox SSL VPN Gateway Web address, such as https://*AccessGatewayFQDN*/
  If a user needs access from a computer that is not running Windows 2000 or above or Linux, but is running a Java Virtual Machine (JVM) 1.4.2 or higher, the user can use the Java applet version of the kiosk. The Web address for connecting to the Java applet version of the kiosk is: https://*AccessGateway*/vpn_portal-javaonly.html
- The authentication realm name required for logon (if you use realms other than the realm named Default).
- Path to any network drives that the users can access, which is done by mapping a network drive on their computer.
- Any system requirements for running the Firebox SSL VPN Gateway Clients if you configured end point resources and policies.

Depending on the configuration of a remote user's system, you might also need to provide additional information:

- To start the Secure Access Client**,** Windows 2000 users must be an administrator to install programs on their computer. This restriction applies to Windows XP for first-time installation only, not for upgrades.
- If a user runs a firewall on the remote computer, the user might need to change the firewall settings so that it does not block traffic to or from the IP addresses to which you granted access. The Secure Access Client automatically handles Internet Connection Firewall in Windows XP and Windows Firewall in Windows XP Service Pack 2. For information about configuring a variety of popular firewalls, see "Using Firewalls with Firebox SSL VPN Gateway" on page 149.
- Users who want to FTP over the Firebox SSL VPN Gateway connection must set their FTP application to perform passive transfers. A passive transfer means that the remote computer establishes the data connection to your FTP server, rather than your FTP server establishing the data connection to the remote computer.
- Users who want to run X client applications across the connection must run an X server, such as XManager, on their computer.

Because users work with files and applications just as if they were local to the organization's network, no retraining of users or configuration of applications is needed.

An email template is provided that includes the information discussed in this section. The template is available from the Downloads page of the Administration Portal. Customize the text for your site and then send the text in an email to users.

Note

To install the Secure Access Client from inside the firewall, go to the portal page and use the **Click here to download the client installer** link to download the client. The first time that the client is run from inside the firewall, point the client to the internal IP address of the Firebox SSL VPN Gateway by right-clicking the Secure Access Client logon and then choosing **Advanced Options**.

Managing Client Connections

The Real-time Monitor lists the open VPN connections by user name and MAC address. For each user, the type of connection by protocol (such as TCP or UDP) is also listed. The Target IP and Target Port provide additional information about the connection. For example, connections to port 21 are FTP connections and connections to port 23 are Telnet connections.

The connections can be managed as follows:

- You can close a connection, such as TCP or UDP.

  For example, suppose that a user has a TCP connection to a Target IP (perhaps a mapped drive) that should be off-limits to the user. You can correct the access control list (ACL) for the user's group and then close the TCP connection. For more information about ACL management, see "Adding Local Users" on page 87. If you do not correct the ACL before closing the connection, the user can reestablish the TCP connection.

Note

The Firebox SSL VPN Gateway maintains connections to Target IP 0.0.0.0 that are required for VPN operations. Closing any of those connections temporarily closes a connection.

- You can disable a user's connection and prevent subsequent logon from that user at the listed MAC address. The user can log on from a different MAC address.
- You can reenable a user name/MAC address combination.

Connection handling

If a user abruptly disconnects the network or puts the computer in hibernate or standby mode, the SSL/TCP connection to the Firebox SSL VPN Gateway is terminated after 10 minutes. A shorter wait period penalizes users who have slow network connections.

This handling of connections results in the following:

- The user might continue to appear active in the Firebox SSL VPN Gateway Real-time Monitor for 10 minutes, after which the connection is terminated.
- The inactive user occupies a license until the wait period expires and the connection is closed. Suppose that you have a license for10 users and all 10 users are logged onto the Firebox SSL VPN Gateway, leaving no available licenses. If one of the active users goes into standby mode, that user's license is not available for 10 minutes.

The wait period does not apply to connections that are terminated through the Real-Time Monitor.

Closing a connection to a resource

Without disrupting a user's VPN connection, you can temporarily close the user's connection to a particular resource. To prevent the user from connecting to the resource, correct the user's group ACL.

To close a connection

1 In the Firebox SSL VPN Gateway Administration Desktop, click the Real-time Monitor icon.

2 Click the arrow to expand the user's entry.

3 Right-click the connection that you want to close and select **Close connection**.

The Firebox SSL VPN Gateway maintains connections to Target IP 0.0.0.0 that are required for VPN operations. Closing any of those connections temporarily closes a connection.

Disabling and enabling a user

The Firebox SSL VPN Gateway tracks user connections by a combination of user name and MAC address, enabling a user to establish simultaneous VPN connections from different computers. You can disable and enable a user and MAC address combination. Disabling a user frees a license.

To disable a user at a particular MAC address

1 In the Administration Desktop, click the Real-time Monitor icon.

2 Right-click the main entry for the user and choose **Disable User from MAC**.

The user cannot establish a connection from that MAC address until you reenable the user or restart the Firebox SSL VPN Gateway.

To enable a user at a particular MAC address

1 In the Administration Desktop window, click the Real-time Monitor icon.

2 Right-click the user's entry and choose **Enable User from MAC**.

The user can establish a connection provided that there is an available license.

Configuring Authentication Requirements after Network Interruption

By default, if a user's network connection is briefly interrupted, the user does not have to log on again when the connection is restored. You can require that users log on after interruptions such as when a computer comes out of hibernation or standby, when the user switches to a different wireless network, or when a connection is forcefully closed.

Note

Note: The Firebox SSL VPN Gateway attempts to authenticate users using the cached password. If users log on using a one-time password, such as used by an RSA SecurID token, authentication on the Firebox SSL VPN Gateway fails, and the user can be locked out and unable to log on.

To prevent the use of one-time passwords, the Firebox SSL VPN Gateway can be configured to force users to log on again after a network interruption. For more information, see "Configuring Authentication to use One-Time Passwords" on page 84.

To require users to log on after a network interruption or on system resume

1 Click the **Access Policy Manager** tab.

2 In the left pane, right-click a group and click **Properties**.

3 On the **General** tab, under **Session options**, select one or both of the following:
- **Authenticate after network interruption.** This option forces a user to log on again if the network connection is briefly interrupted.
- **Authenticate upon system resume.** This option forces a user to log on again if the user's computer awakens from standby or hibernation. This option provides additional security for unattended computers.

4 Click **OK**.

Note

Note: If you want to close a connection and prevent a user or group from reconnecting automatically, you must select the **Authenticate after network interruption** setting. Otherwise, users immediately reconnect without being prompted for their credentials.

APPENDIX A

Firebox SSL VPN Gateway Monitoring and Troubleshooting

The following topics describe how to use Firebox SSL VPN Gateway logs and troubleshoot issues:

- Viewing and Downloading System Message Logs
- Enabling and Viewing SNMP Logs
- Viewing System Statistics
- Monitoring Firebox SSL VPN Gateway Operations
- Recovering from a Failure of the Firebox SSL VPN Gateway
- Troubleshooting

Viewing and Downloading System Message Logs

There are two types of logging for the Firebox SSL VPN Gateway. All of the logs are stored locally and can be viewed from either the Administration Tool or the Administration Portal. Optionally, this same information can be sent to a syslog server.

System message logs contain information that can help Firebox SSL VPN Gateway support personnel assist with troubleshooting. By reviewing the information provided, you can track unusual changes that can affect the stability and performance of the Firebox SSL VPN Gateway.

System message logs are archived on the Firebox SSL VPN Gateway for 30 days. The oldest log is then replaced with the current log.

You can download one or all logs at any time. You can also have system messages forwarded to your syslog server, as described in "Forwarding System Messages to a Syslog Server" on page 138.

Note

If you need to view the system log and the Firebox SSL VPN Gateway is offline, go to the Administration Portal and click the **Logging** tab.

To view and filter the system log

1 In the Administration Tool, click the **VPN Gateway Cluster** tab.

2 Open the tab for the Firebox SSL VPN Gateway.

3 Click **Logging/Settings.**

4 Under **Gateway Log**, click **Display Logging Window**.
The log for today's date is displayed.
To display the log for a prior date, select the date in the **Log Archive** list and click **View Log**.

5 By default, the log displays all entries. The log can be filtered as described below:
- To filter the log by user or applications, under **Log Filter**, select **Admins**, **Apps**, or **Users**.
- To filter the log by priority, under **Log Filter**, select **LO**, **MED**, **HI**, or **CRIT**.
- The filters that you select are treated as logical ORs. Thus, for each selected filter, all matches for the filter are displayed.

6 To download a log:
- Select a log in the Log Archive list and next to **Selected Log File,** click **Download**. The log filename defaults to *yyyymmdd*.log.
- To download all of the logs, next to **All Log Files**, click **Download**. The filename defaults to log_archive_*yyyymmdd*.tgz. To download logs from the Firebox SSL VPN Gateway, you must have a data compression utility, such as WinZip, installed on your computer. The logs are downloaded as .tgz files and that data must be extracted. After the file downloads, it can be unzipped to access the individual log files.

Forwarding System Messages to a Syslog Server

The Firebox SSL VPN Gateway archives system messages, as described in "Viewing and Downloading System Message Logs" on page 137. You can also have the Firebox SSL VPN Gateway forward system messages to a syslog server.

To forward Firebox SSL VPN Gateway system messages to a syslog server

1 Click the **VPN Gateway Cluster** tab and then click the **Logging/Settings** tab.

2 Under **Syslog Settings**, in **Server**, type the IP address of the syslog server.

3 In **Facility**, select the syslog facility level.

4 In **Broadcast Interval (mins)**, type a broadcast frequency in minutes. If the broadcast frequency is set to 0, logging is continuous.

5 Click **Submit**.

Viewing the W3C-Formatted Request Log

The Firebox SSL VPN Gateway logs incoming and outgoing HTTP requests in the W3C extended log format. You can analyze the log by using a conventional log file analysis tool.

The log contains the following fields::

Field	Description
date	Date of access, specified in GMT and formatted as YYYY-MM-DD
time	Time of access, specified in GMT and in 24-hour format, HH:MM:SS.
c-ip	Client IP address.
cs-method	The client-to-Firebox SSL VPN Gateway request method, either GET or POST.
sc-method	The Firebox SSL VPN Gateway-to-client request method, either GET or POST.

Field	Description
sc-status	The Firebox SSL VPN Gateway-to-client request status code. For a description of status codes, refer to http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html.
cs-uri	The client-to-Firebox SSL VPN Gateway request URI.
sc-uri	The Firebox SSL VPN Gateway-to-client request URI.

To view or download the log, go to the **Logging > Configuration** tab and click **Download W3C Log**.

Enabling and Viewing SNMP Logs

When Simple Network Management Protocol (SNMP) is enabled, the Firebox SSL VPN Gateway reports the MIB-II system group (1.3.6.1.2.1). The Firebox SSL VPN Gateway does not support Firebox SSL VPN Gateway-specific SNMP data.

You can view SNMP messages in the Administration Tool and you can configure an SNMP monitoring tool such as the Multi Router Traffic Grapher to provide a visual representation of the SNMP data reported by the Firebox SSL VPN Gateway in response to queries. For a sample of Traffic Grapher output, see "Multi Router Traffic Grapher Example" on page 139.

To enable logging of SNMP messages

1 Click the **VPN Gateway Cluster** tab and then click the **Logging/Settings** tab.
2 Under **SNMP Settings**, select **Enable SNMP**.
3 In **SNMP Location,** type the SNMP location. This field is informational only.
4 In **SNMP Contact,** type the contact. This field is informational only.
5 In **Community**, type the community. This field is informational only.
6 In **Port**, type the port.
7 Click **Submit**.

Multi Router Traffic Grapher Example

The Multi Router Traffic Grapher is a tool used to monitor SNMP data, such as traffic load. Multi Router Traffic Grapher generates HTML pages containing PNG images that provide a visual representation of the traffic. Multi Router Traffic Grapher works under UNIX, Windows 2000 Server, and Windows Server 2003.

Note

The information in this section provides a general overview of working with Multi Router Traffic Grapher. For information about obtaining and using this tool, visit the Multi Router Traffic Grapher Web site at http://people.ee.ethz.ch/~oetiker/webtools/mrtg/.

To obtain SNMP data for the Firebox SSL VPN Gateway through Multi Router Traffic Grapher (in UNIX)

1 Configure the Firebox SSL VPN Gateway to respond to SNMP queries as discussed in "To enable logging of SNMP messages" on page 139.

2 Create Multi Router Traffic Grapher configuration files in /etc/mrtg.

Each configuration file specifies the object identifiers that the grapher daemon is to monitor, specifies the target from which to obtain SNMP data, and defines the grapher output.

```
WorkDir: /var/www/html/mrtg
Options[_]: nopercent,gauge,noinfo,growright

Target[vpn.myorg.com.tcpCurrEstab]: .1.3.6.1.2.1.6.9.0&.1.3.6.1.2.1.6.9.0:mypswd@10.10.0.30
Xsize[vpn.myorg.com.tcpCurrEstab]: 600
Ysize[vpn.myorg.com.tcpCurrEstab]: 200
Ytics[vpn.myorg.com.tcpCurrEstab]: 10
Title[vpn.myorg.com.tcpCurrEstab]: ESTABLISHED TCP connections
PageTop[vpn.myorg.com.tcpCurrEstab]: <h1>ESTABLISHED TCP connections</h1>
MaxBytes[vpn.myorg.com.tcpCurrEstab]: 1000000
YLegend[vpn.myorg.com.tcpCurrEstab]: # est. conns
ShortLegend[vpn.myorg.com.tcpCurrEstab]:  
LegendI[vpn.myorg.com.tcpCurrEstab]:  Connections: 
LegendO[vpn.myorg.com.tcpCurrEstab]:
Legend1[vpn.myorg.com.tcpCurrEstab]: Established TCP connections
```

The Multi Router Traffic Grapher configuration file

3 Modify /etc/crontab to perform an SNMP query every five minutes, resulting in graphed data. The various .cfg files listed generate a separate output.

4 View the output in a Web browser.

The grapher stores HTML output in the Workdir specified in the configuration file. The output filename that corresponds to the configuration file in Step 2 is vpn.myorg.com.tcpcurrestab.html.

Viewing System Statistics

To obtain general system statistics, select the **VPN Gateway Cluster** tab and then click the **Statistics** tab.

The statistical information provides an overview of the Firebox SSL VPN Gateway and includes:

- Length of time the Firebox SSL VPN Gateway has been running.
- Memory usage.
- Maximum and used connections. Maximum connections represent the number of licenses that are available for use with the Firebox SSL VPN Gateway.
- Logon information for both the full client and kiosk clients.

Monitoring Firebox SSL VPN Gateway Operations

The Firebox SSL VPN Gateway includes a variety of standard Linux monitoring applications so that you can conveniently access the applications from one location. With the exception of the Real-time Monitor, written by Firebox SSL, the applications are included in the Firebox SSL VPN Gateway under the GNU public license.

The monitoring applications are located in the Firebox SSL VPN Gateway Administration Desktop. The icons across the bottom left of the screen provide single-click access to the six monitoring tools. In the

bottom right corner, you can view process and network activity levels; mouse over the two graphs to view numeric data.

To open the Firebox SSL VPN Gateway Administration Desktop

1 Open a Web browser and type the IP address or FQDN of the Firebox SSL VPN Gateway. The accepted formats are *https://IPaddress* or *https://FQDN***.**

2 In the Firebox SSL VPN Gateway Administration Portal, click **Downloads**.

3 Under **Administration**, click **Launch Firebox SSL VPN Gateway Administration Desktop**.

The monitoring applications are as follows.

Firebox SSL Real-time Monitor

Shows the open client connections. To view details about a connection, click the arrow for the user name.

From the monitor, you can temporarily close a connection by connection type (TCP and so on), disable a user (the user cannot connect until you enable the user), and enable a user again. For more information, see "Managing Client Connections" on page 133.

Ethereal Network Analyzer

Enables you to interactively browse packet data from a live network or from a previously saved capture file. For more information, refer to the Help that is available from the Ethereal Network Analyzer window.

xNetTools

Multi-threaded network tool that includes a service scanner, port scanner, ping utility, ping scan, name scan, whois query, and finger query. This is located on the **Tools** menu.

Traceroute

Combines the functionality of the traceroute and ping commands in one network diagnostic tool. As Traceroute starts, it investigates the network connection between the Firebox SSL VPN Gateway and the destination host that you specify. After it determines the address of each network hop between the devices, it sends a sequence ICMP ECHO request to each one to determine the quality of the link to each device. As it does this, it prints running statistics about each device.

fnetload

Provides real-time network interface statistics. It checks the /proc/net/dev every second and builds a graphical representation of its values.

System Monitor

Shows information about CPU usage and memory/swap usage. For more information, refer to the Help available from the System Monitor window.

Recovering from a Failure of the Firebox SSL VPN Gateway

In the event of a total system failure, you must do four procedures to recover:

- reinstall the v 4.9 software on your Firebox® SSL Core appliance
- back up your configuration settings
- apply the v 5.0 software update

- apply the v 5.5 software update

Reinstalling v 4.9 application software

To reinstall v 4.9 on your appliance:

1 Find the Firebox® SSL v 4.9.2 Recovery CD that came with your original Firebox® SSL Core appliance.

2 Use the instructions in the v 4.9 Administration Guide starting on page 153 to reinstall your application software with the system CD.

Backing up your configuration settings

Before starting the v 5.0 software update process, be sure to back up your configuration settings.

1 In the v 4.9 Administration Tool, click the **Access Gateway Cluster** tab.

2 Open the dialog box for the appliance.

3 On the **Administration** tab, click **Save Configuration** (this option appears near the option **Save the current configuration).**

4 Save the file, named **config.restore**, to your computer.
For more information about creating backup files, see page 47 of the v 4.9 Administration Guide.

Upgrading to SSL v 5.0

To obtain the v 5.0 software update, v 5.0 Administrator's Guide and v 5.0 Release Notes, go to *https://www.watchguard.com/archive/softwarecenter.asp*. You must log in with your LiveSecurity user name and passphrase and select the Firebox SSL VPN Gateway support view.

From your current Firebox SSL VPN Gateway running v 4.9, you can upgrade to SSL v 5.0 in one of two ways:

- From the v 4.9 Administration Tool Interface, go to the **Administration** tab and **Maintenance** sub tab. Click on the **Browse** button for **Upload a server Upgrade or saved config**.

or

- From the v 4.9 Administration Portal web page, go to the **Maintenance** tab and click **Browse** for the **Upload Server Upgrade or Server Config** option.

After you upgrade your Firebox® SSL VPN Gateway and re-connect to the Administration Portal, select the option **Download Access Gateway Administration Tool**. Double-click the citrix_admin_monitor.exe file to install the executable.

Note

Make sure that the v 4.9 Administration Tool has been uninstalled using Control Panel > Add/Remove Programs.

Upgrading to SSL v 5.5

To obtain the v 5.5 software update, v 5.5 Administrator's Guide and v 5.5 Release Notes, go to *https://www.watchguard.com/archive/softwarecenter.asp*. You must log in with your LiveSecurity user name and passphrase and select the Firebox SSL VPN Gateway support view.

To upgrade to v 5.5.

1 In the v5.0 Administration Tool, click the **Firebox® SSL VPN Gateway Cluster** tab.
2 On the **Administration** tab, next to **Upload a server upgrade or saved config**, click **Browse**.
3 Navigate to the upgrade file and click **Open**.
4 Wait for the message **Upgrade successful** to appear and then restart the device.

Note: If the upgrade file has the extension .zip, extract the files before you upgrade the Firebox® SSL VPN Gateway.

Launching the v 5.5 Administration Tool

After the Administration Tool installation is complete, you can launch the new tool from **Start > All Programs > WatchGuard**. Type the IP address or FQDN of the SSL VPN Gateway device in the Connecting To dialog box. Note that the dialog box does not always appear in the foreground—it may be buried behind other open windows on your desktop.

Note

Both ports 9001 and 9002 are required for administrator traffic. This is detailed in Chapter 2, "Introduction to Firebox SSL VPN Gateway." .

You may need to log in to your LiveSecurity account at *https://www.watchguard.com/archive/getcredentials.asp* to get a copy of your feature key..

Troubleshooting

The following information explains how to deal with problems you might encounter when setting up and using the Firebox SSL VPN Gateway.

Troubleshooting the Web Interface

This section describes issues you might have with connecting to the Web Interface.

Web Interface Appears without Typing in Credentials

If you typed the Web address for the Firebox SSL VPN Gateway, the Web Interface appears without asking for the user name and password. The problem is that you have portal page authentication disabled. In the Administration Tool, on the **Global Cluster Policies** tab, under **Advanced Options**, select **Enable Portal Page Authentication**.

If this is disabled, unauthenticated network traffic is sent to the Web Interface. This is a valid configuration; however, make sure the Web Interface is located in the DMZ.

Applications do not Appear after Logging On

When users log on to the Firebox SSL VPN Gateway, they cannot see their applications. The Message Center states that a domain was not specified.

By default, the Firebox SSL VPN Gateway passes only the user name and password to the Web Interface. To correct this, configure a default domain or a set of domains users can log on to. The Web Interface uses the first one in the list as the default domain.

Web Interface Credentials Are Invalid

When users log on to the Firebox SSL VPN Gateway, they are sent to the Web Interface but their applications are not displayed. The Message Center states that the users' credentials are invalid.

The most likely cause of this error message is that the users logged onto the Firebox SSL VPN Gateway with non-LDAP credentials from a different domain than the Web Interface is set up to accept. To resolve this issue, make sure that the default domain on the server running the Web Interface is the same as the default realm in the Firebox SSL VPN Gateway.

Users could also log on using a realm in the Firebox SSL VPN Gateway but the realm name does not correspond to a domain name that is supported by the Web Interface. To allow users to log on with a realm name, type the realm name after the domain in Active Directory. When users log on to the Firebox SSL VPN Gateway, the realm name and user name are passed to the Web Interface. The Web Interface converts the realm name and user name to the domain name and user name.

Other Issues

This section describes known issues and solutions for the Firebox SSL VPN Gateway.

License File Does not Match Firebox SSL VPN Gateway

If you are trying to install a license file on the Firebox SSL VPN Gateway, you might receive the error message "License file does not match any Firebox SSL VPN Gateway's." A license file is already installed on the Firebox SSL VPN Gateway. To upload a new license file, the old license needs to be removed.

To install a new license file on the Firebox SSL VPN Gateway

1 Open the Administration Tool.

2 On the **VPN Gateway Cluster** tab, select the Firebox SSL VPN Gateway to which you want to add the license.

3 On the **Licensing** tab, next to **Clear all licensing**, click **Remove All**.

4 Restart the Firebox SSL VPN Gateway.

5 On the **Licensing** tab, next to **Upload a license file**, click **Browse** and navigate to the license file.

6 Click **Open** to install the file.

7 Restart the Firebox SSL VPN Gateway.

Read/Write Access to the Firebox SSL VPN Gateway

If a user is using a signed Java applet, it is possible to read and write files to the Firebox SSL VPN Gateway's local disk in a restricted area. This can be prevented by doing one of the following:

- Disabling connections from a public computer
- Allowing connections from a public computer but disabling Firefox
- Allowing connections from a public computer with Firefox but configuring the correct Access Control policies that prevent Firefox from accessing any Web site that contains a signed Java applet

Defining Accessible Networks

In the **Accessible Networks** field on the **Global Cluster Policies** tab, up to 24 subnets can be defined. If more than 24 subnets are entered, the Firebox SSL VPN Gateway ignores the additional subnets.

VMWare

If a user logs on to the Secure Access Client from two computers that are running VMWare and VMWare uses the same MAC address for the two computers, the Firebox SSL VPN Gateway does not allow both clients to run simultaneously. The Firebox SSL VPN Gateway uses the MAC address to manage licenses and does not allow more than one client session at a time per MAC address.

ICMP Transmissions

The Firebox SSL VPN Gateway returns a "Request timed out" error message if an ICMP transmission fails for any reason. The Firebox SSL VPN Gateway always sends a standard ICMP packet to the remote destination host when a client tries to ping it. Any client options such as increasing the size of the ICMP payload are not recognized by the Firebox SSL VPN Gateway and are not sent to the remote host.

Ping Command

The Firebox SSL VPN Gateway always sends out the same ping command, regardless of the options specified with the ping command from a client computer.

LDAP Authentication

When the Firebox SSL VPN Gateway is configured to use LDAP authentication and authorization, the LDAP group information is not used to automatically populate the group field in the Administration Tool.

End Point Policies

When the Firebox SSL VPN Gateway is evaluating the union of a group's end point policies, it does not consider the group priorities and therefore might not resolve conflicting policies correctly. The last policy appended in an expression is the policy that takes effect. For example, one group has policy ProcessA and another group has policy !ProcessA. If the union of the policies is ProcessA and !ProcessA, the !ProcessA takes effect.

Network Resources

For added network resources, the Firebox SSL VPN Gateway does not recognize the CIDR notation address *ipaddress*/0. For example, to add a resource group that provides access to all resources, specify 0.0.0.0/0.0.0.0 instead of 0.0.0.0/0.

Kiosk Connections

For kiosk connections, the Firebox SSL VPN Gateway must have a certificate that is signed by a Sun Microsystems trusted Certificate Authority.

Client connections using kiosk mode require the installation of Java Runtime Environment (JRE) 1.4+ on their computer.

Internal Failover

If internal failover is enabled and the administrator is connected to the Firebox SSL VPN Gateway, the Administration Tool cannot be reached over the connection. To fix this problem, enable IP pooling and then connect to the lowest IP address in the pool range on port 9001. For example, if the IP pool range starts at 10.10.3.50, connect to the Administration Tool using 10.10.3.50:9001. For information about configuring IP pools, see "Enabling IP Pooling" on page 94.

Certificate Signing

There are several server components that support SSL/TLS, such as the Firebox SSL VPN Gateway, Secure Gateway, and SSL Relay. All of these components support server certificates issued either by a public Certificate Authority (CA) or by a private Certificate Authority. Public CAs include organizations such as Verisign and Thawte. Private CAs are implemented by products such as Microsoft Certificate Services.

Certificates signed by a private CA are sometimes described as *enterprise certificates* or *self-signed certificates*. In this context, the term self-signed certificate is not technically accurate; such certificates are signed by the private CA. True self-signed certificates are not signed by any CA and are not supported by the server components, because there is no CA to provide a root of trust. However, as described above, certificates issued by a private CA are supported by the server components because the private CA is the root of trust.

Certificate Revocation Lists

Certificate Revocation Lists (CRLs) cannot be configured by the administrator. When a user connects to the Firebox SSL VPN Gateway using a client certificate, the Firebox SSL VPN Gateway uses the cRLDistributionPoints extension in the client certificate, if it is present, to locate relevant CRLs using HTTP. The client certificate is checked against those CRLs.

Retrieving CRLs using LDAP is not supported.

Network Messages to Non-Existent IPs

If an invalid sdconf.rec file is uploaded to the Firebox SSL VPN Gateway, this might cause the Firebox SSL VPN Gateway to send out messages to non-existent IPs. A network monitor might flag this activity as network spamming.

To correct the problem, upload a valid sdconf.rec file to the Firebox SSL VPN Gateway.

The Firebox SSL VPN Gateway Does not Start and the Serial Console Is Blank

Verify that the following are correctly set up:

- The serial console is using the correct port and the physical and logical ports match
- The cable is a null-modem cable
- The COM settings in your serial communication software are set to 9600 bits per second, 8 data bits, no parity, and 1 stop bit

The Administration Tool Is Inaccessible

If the Firebox SSL VPN Gateway is offline, the Administration Tool is not available. You can use the Administration Portal to perform tasks such as viewing the system log and restarting the Firebox SSL VPN Gateway.

Devices Cannot Communicate with the Firebox SSL VPN Gateway

Verify that the following are correctly set up:

- The External Public Address specified on the **General Networking** tab in the Firebox SSL VPN Gateway Administration Tool is available outside of your firewall
- Any changes made in the Firebox SSL VPN Gateway serial console or Administration Tool were submitted

Using Ctrl-Alt-Delete to Restart the Firebox SSL VPN Gateway Fails

The restart function on the Firebox SSL VPN Gateway is disabled. You must use the Firebox SSL VPN Gateway Administration Tool to restart and shut down the device.

SSL Version 2 Sessions and Multi-Level Certificate Chains

If intermediate (multi-level) certificates are part of your secure certificate upload, make sure that the intermediate certificates are part of the certificate file you are uploading. SSL Version 2 does not support certificate chaining. Any certificate that has more than one level must include all intermediate certificates or the system may become unusable. For information about how to add intermediate certificates to the uploaded certificate file, see "Generating Trusted Certificates for Multiple Levels" on page 156.

H.323 Protocol

The Firebox SSL VPN Gateway does not support the H.323 protocol. Applications that use the H.323 protocol, such as Microsoft's NetMeeting, cannot be used with the Firebox SSL VPN Gateway.

Certificates Using 512-bit keypairs

When configuring certificates, do not use 512-bit keypairs. They are subject to brute force attacks.

Secure Access Client

The following are issues with the Secure Access Client.

Secure Access Client Connections with Windows XP

If a user makes a connection to the Firebox SSL VPN Gateway using Windows XP, logs off the computer without first disconnecting the Secure Access Client, and then logs on again, the Internet connection is broken. To restore the Internet connection, restart the computer.

DNS Name Resolution Using Named Service Providers

If clients without administrative privileges use Windows 2000 Professional or Windows XP to connect to the Firebox SSL VPN Gateway, DNS name resolution may fail if the client is using the Name Service Provider. To correct the problem, connect using the IP address of the computer instead of the DNS name.

Auto-Update Feature

The Secure Access Client auto-update feature does not work if the client is configured to connect through a proxy server.

Client Connections from a Windows Server 2003

If a connection to the Firebox SSL VPN Gateway is made from a Windows Server 2003 computer that is its own DNS server, local and public DNS resolution does not work. To fix this issue, configure the Windows Server 2003 network settings to point to a different DNS server.

NTLM Authentication

The Secure Access Client does not support NTLM authentication to proxy servers. Only Basic authentication is supported for proxy servers.

WINS Entries

When the Secure Access Client is disconnected, WINS entries are not removed from the computer that is running the client.

Using Third-Party Client Software

If a user's computer is running Secure Access Client, and also has a third-party VPN software application installed on the computer, and connections are not correctly crossing the Firebox SSL VPN Gateway, make sure the third-party application is disabled or turned off. When the third-party application is disabled or off, try the Firebox SSL VPN Gateway connection again.

APPENDIX B

Using Firewalls with Firebox SSL VPN Gateway

If a user cannot establish a connection to the Firebox SSL VPN Gateway or cannot access allowed resources, it is possible that the firewall software on the user's computer is blocking traffic. The Firebox SSL VPN Gateway works with any personal firewall, provided that the application allows the user to specify a trusted network or IP address for the Firebox SSL VPN Gateway.

This section discuss the following popular firewalls and configuration instructions for them.

- BlackICE PC Protection
- McAfee Personal Firewall Plus
- Norton Personal Firewall
- Sygate Personal Firewall (Free and Pro Versions)
- Tiny Personal Firewall
- ZoneAlarm Pro

Note

The following sections are a supplement to the firewall manufacturer's documentation. The recommended source for current information about firewall applications and configuration is the manufacturer's documentation.

WatchGuard recommends that the user's personal firewall allow full access for the Secure Access Client. If you do not want to allow full access, the following UDP and UDP/TCP ports need to be open on the client computer:

- 10000 (UDP)
- 10010 (UDP/TCP)
- 10020 (UDP)
- 10030 (UDP)

Personal firewalls need to be configured to allow traffic to and from the Firebox SSL VPN Gateway IP address or FQDN. To find out which ports are open, use the Secure Access Client **Properties** page that is accessible from the connection icon in the notification tray. The ports that are open are listed on the **Details** tab.

To view Secure Access Client status properties

Double-click the Secure Access Client connection icon in the notification area. Alternatively, right-click the icon and choose **Properties** from the menu.

The **Secure Access Client** dialog box appears.

The properties of the connection provide information that is helpful for troubleshooting. The properties include:

- The **General** tab displays connection information.
- The **Details** tab displays server information and a list of the secured networks clients are allowed to access.
- The **Access Lists** tab displays the access control lists (ACLs) that are configured for the user connection. This tab does not appear for users who are not in a group or if an ACL is not configured for a group.

The following are suggestions for using some popular firewalls with the Firebox SSL VPN Gateway.

BlackICE PC Protection

The following BlackICE settings enable the Secure Access Client to reach the Internet and the resources allowed by the Firebox SSL VPN Gateway. To configure the settings, open the BlackICE window and choose the following commands.

Tools > **Edit** BlackICE Settings	On the **Firewall** tab, make sure that the Protection Level is lower than "Paranoid," which prevents you from running applications, such as email, over the connection. On the **Intrusion Detection** tab, add the IP address of the Firebox SSL VPN Gateway as a trusted zone. Also add the IP address or range of allowed resources as trusted zones. When you add an IP address, be sure to select the **Add Firewall Entry** check box.

McAfee Personal Firewall Plus

The following McAfee Personal Firewall Plus settings enable the Secure Access Client to reach the Internet and the resources allowed by the Firebox SSL VPN Gateway. To configure the settings, open the McAfee Security Center window, click the **Personal Firewall+** tab, and choose the following commands.

The following settings assume that you are using the Standard security level. To check your security level, go to the **Personal Firewall+** tab, click **Utilities**, and then click **Security Settings**.

Note

By default, when the Secure Access Client is installed, Personal Firewall Plus prompts you to grant or block access for the application. Select **Grant Access**.

.

Trusted & Banned IPs	Add the IP address or range of allowed resources as trusted IP addresses.
System Services	In the System Services list, select each service that you plan to use over the VPN connection.

Norton Personal Firewall

If you are using the default Norton Personal Firewall settings, you can simply respond to the Program Control alerts the first time that you attempt to start the Secure Access Client or when you access a blocked location or application. When you respond to such an alert, choose the **Permit** action, select **Always use this action**, and click **OK**.

If you changed the default firewall settings, you might need to manually configure the following settings to reach the Internet and the resources allowed by the Firebox SSL VPN Gateway. To configure the settings, open the Norton Personal Firewall window and choose the following tabs.

Networking	You might need to add the following as trusted zones: - The IP address of the Firebox SSL VPN Gateway - The IP address or range of allowed resources Click **Add** and enter the IP address(es).
Programs	You might need to grant access to individual applications. Click **Add** and then browse for and select the application. When prompted, choose **Permit**.

Sygate Personal Firewall (Free and Pro Versions)

Each time the Sygate Personal Firewall encounters new activity for which it does not have a rule, it displays a prompt. To grant access to the applications and locations that you will access through the Secure Access Client, select the **Remember my answer** check box and click **Yes** when the prompt appears.

Tiny Personal Firewall

The following Tiny Personal Firewall settings enable the Secure Access Client to reach the Internet and the resources allowed by the Firebox SSL VPN Gateway.

Note

One method to configure Tiny Personal Firewall is to respond to the prompts displayed when the firewall encounters new activity for which it does not have a rule. The following information assumes that Tiny Personal Firewall is configured before installing the Secure Access Client.

To configure the settings, open the Tiny Personal Firewall administration window, click the **Advanced** button to view the Firewall Configuration window, and then use the **Filter Rule** dialog box as indicated below.

Add	To permit the IP address or range of allowed resources, use the following settings: Protocol = **TCP and UDP** Direction = **Both Directions** Local Endpoint fields = **Any** Remote Endpoint = specify IP address(es) Action = **Permit**

After you apply the above configuration and start the Secure Access Client, Tiny Personal Firewall displays several Incoming Connection Alerts related to the Secure Access Client. For each alert, select the **Create appropriate filter** check box and click **Permit**.

ZoneAlarm Pro

The following ZoneAlarm settings enable the Secure Access Client to reach the Internet and the resources allowed by the Firebox SSL VPN Gateway. To configure the settings, choose the tabs indicated in the following table.

Firewall > Zones	Define the host name of the Firebox SSL VPN Gateway as a trusted zone.

APPENDIX C

Installing Windows Certificates

The Firebox SSL VPN Gateway includes the Certificate Request Generator to automatically create a certificate request. After the file is returned from the Certificate Authority, it can be uploaded to the Firebox SSL VPN Gateway. When the file is uploaded, it is converted automatically to the correct format for use.

If you do not want to use the Certificate Request Generator to create the signed certificate, use Linux OpenSSL to administer any certificate tasks. If Linux is not available, Cygwin UNIX environment for Windows is recommended, which includes an OpenSSL module. Instructions for downloading, installing, and using the Cygwin UNIX environment to generate a CSR are included in this section.

If you are familiar with certificate manipulation, you can use other tools to create a PEM-formatted file. The certificate that you upload to the Firebox SSL VPN Gateway must have the following characteristics:

- It must be in PEM format and must include a private key
- The signed certificate and private key must be unencrypted

If Linux OpenSSL is not available, install the Cygwin UNIX environment for Windows. When you install Cygwin, you must choose the OpenSSL modules as described in the following steps.

To install Cygwin

1. Use a Web browser to navigate to http://www.cygwin.com and click **Install Cygwin Now**.
2. Follow the on-screen instructions to open the setup installer.
3. In the **Cygwin Setup** dialog box, click **Next**.
4. Click **Install from Internet** and then click **Next**.
5. Accept the default root installation directory settings and then click **Next**.
6. Accept the default local package directory setting and then click **Next**.
7. In the **Internet Connection** screen, click **Use IE5 Settings** and then click **Next**.
8. In the list of Available Download Sites, click **ftp://ftp.nas.nasa.gov** and then click **Next**.
9. In the **Select Packages** screen, click the **View** button.
10. Scroll the packages list to locate in the Package column **openssl: The OpenSSL runtime environment** and **openssl-devel: The OpenSSL development environment**.
11. In the **New** column for those two entries, click **Skip**.
    The current version number of Cygwin appears.

12 Click **Next** to start the installation.

After Cygwin installs, you can generate the CSR.

These instructions to generate a CSR assume that you are using the Cygwin UNIX environment installed as described in "To install Cygwin" on page 153.

To generate a CSR using the Cygwin UNIX environment

1 Double-click the **Cygwin** icon on the desktop.
A command window opens with a UNIX bash environment.

2 To change to a particular drive, use the command: **cd driveLetter:**

3 At the $ prompt, type the following to generate a CSR:

openssl req -new -nodes -keyout *privateKeyFilename* **-out** *certRequestFilename*

For example:

openssl req -new -nodes -keyout private.key -out public.csr

Status messages about the private key generation appear. You are prompted for information such as country name.

4 When prompted for the Common name, enter the DNS name of the Firebox SSL VPN Gateway.

The name that you enter appears on the certificate and must match the name expected by computers that connect to the Firebox SSL VPN Gateway. Thus, if you alias DNS names, you need to use the alias name instead.

5 Submit your CSR (public.csr) to an authorized Certificate Authority such as Verisign. When asked for the type of server that the certificate will be used with, select Apache.

Note

If you select "Microsoft," the certificate might be in PKCS7 format and you will need to follow the procedure in "Converting to a PEM-Formatted Certificate" on page 155 to convert the certificate to a PEM format.

Unencrypting the Private Key

The following procedure is not needed if you use the Cygwin UNIX environment to generate the CSR and private key. Follow this procedure only if the method you use to generate the private key results in an encrypted key.

To unencrypt the private key

1 At the $ prompt enter the command: **openssl rsa**

If you enter this command without arguments, you are prompted as follows:

read RSA key

2 Enter the name of the password to be encrypted.

You can enter the **openssl rsa** command with arguments if you know the name of the private key and the unencrypted PEM file.

For example, if the private key filename is **my_keytag_key.pvk** and the unencrypted filename is **keyout.pem**, enter **openssl rsa -in my_keytag_key.pvk -out keyout.pem**.

For more information, see the Open SSL Web site at http://www.openssl.org/docs/apps/rsa.html#EXAMPLES.

For information about downloading OpenSSL for Windows, see the SourceForge Web site at http://sourceforge.net/project/showfiles.php?group_id=23617&release_id=48801.

Converting to a PEM-Formatted Certificate

The signed certificate file that you receive from the Certificate Authority might not be in a PEM format. If the file is in binary format (DER), convert it to PEM format as follows:

openssl x509 -in *certFile* **-inform DER -outform PEM -out** *convertedCertFile*

If the certificate is already in a text format, it may be in PKCS format. You will receive a PKCS formatted certificate if you specified that the certificate will be used with a Microsoft rather than Apache operating system. The following command results in an error message if the certificate is not in PEM format. The *certFile* should not contain the private key when you run this command.

openssl verify -verbose -CApath /tmp *certFile*

If that command results in the following error message, the file is not in PEM format.

certFile: unable to load certificate file
4840:error:0906D064:PEM routines:PEM_read_bio:bad base64
decode:pem_lib.c:781:

To convert the certificate from PKCS7 to PEM format

1 Run the command:

openssl pkcs7 -in ./*certFile* **-print_certs**

The output will look like this:

subject=...
...
-----BEGIN CERTIFICATE-----
... Server Certificate ...
-----END CERTIFICATE-----
subject=...
...
-----BEGIN CERTIFICATE-----
... Intermediate Cert ...
-----END CERTIFICATE-----

2 Combine the server certificate data and the intermediate certificate data (if it exists) from the output with the private key as specified in "Combining the Private Key with the Signed Certificate" on page 155 and "Generating Trusted Certificates for Multiple Levels" on page 156.

Combining the Private Key with the Signed Certificate

You must combine the signed certificate with the private key before you can upload it to the Firebox SSL VPN Gateway.

To combine the private key with the signed certificate

1 Use a text editor to combine the unencrypted private key with the signed certificate in the PEM file format.

The file contents should look similar to the following:

-----BEGIN RSA PRIVATE KEY-----

<Unencrypted Private Key>

-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----

<Signed Certificate>

-----END CERTIFICATE-----

2 Save and name the PEM file; for example, **AccessGateway.pem**.

Generating Trusted Certificates for Multiple Levels

Note

You must determine whether or not your certificate has more than one level and, if it does, handle the intermediate certificates properly.

To generate trusted certificates for multiple levels

1 Open Internet Explorer and access a Web page through the Firebox SSL VPN Gateway. For example, enter an address similar to the following:

https://*ipAddress***:***httpPort***//www.***mypage***.com**

where:

ipAddress is the IP address of your Firebox SSL VPN Gateway

httpPort is the Firebox SSL VPN Gateway port number

2 Double-click the Lock symbol in the bottom right corner of the browser.

3 Switch to the Certificate Path window pane at the top of the screen.

4 Double-click the first path level to bring up the certificate information for the first level and then go to the **Details** screen.

5 Click the **Copy to File** button at the bottom.

6 After the Certificate Export wizard appears, click **Next**.

7 Click the format **Base-64 encoded** and then click **Next**.

8 Enter a filename; for example, G:\tmp\root.cer.

9 Review the information and note the complete filename. Click **Finish**.

10 Click **OK** to close the **Certificate Information** window for the first level.

11 Repeat Steps 4–10 for all levels except the last level.

12 Insert all certificates into one file and make sure that any intermediate certificates are part of any certificate file you upload.

The file to be uploaded should be in the following format:

private key
Server Certificate

Intermediate Certificate 0
Intermediate Certificate 1
Intermediate Certificate 2

APPENDIX D

Examples of Configuring Network Access

After the Firebox SSL VPN Gateway is installed and configured to operate in your network environment, use the Administration Tool to configure user access to the servers, applications, and other resources on the internal network.

Configuring user access to internal network resources involves defining accessible networks for split tunneling, configuring authentication and authorization, creating user groups, creating local users, and defining the access control lists (ACLs) for user groups.

Note

An ACL is a set of policies that determines the level of access that users have to the network resources.

The Firebox SSL VPN Gateway supports several different authentication and authorization types that can be configured in a variety of combinations and used with policies to control user access to the internal network.

Because of the number of options and possibilities involved with configuring user access to the internal network, this aspect of Firebox SSL VPN Gateway configuration is covered in four different sections of this book.

- This appendix provides example user access scenarios and includes step-by-step instructions for configuring the Firebox SSL VPN Gateway to support the access scenarios. These scenarios are intended as tutorials to help you understand how to use the features of the Administration Tool to configure user access, and are not examples of real-world configurations.
  After you read these examples and understand the basics of configuring user access, use the information provided in the three chapters listed below to complete your configuration.
- "Configuring Authentication and Authorization" on page 61". This chapter discusses the different authentication and authorization options and how to configure them.
- "Adding and Configuring Local Users and User Groups" on page 87. This chapter discusses how to work with user groups, network resources, and various policies to define access control lists (ACLs) on the Firebox SSL VPN Gateway.
- "Working with Client Connections" on page 117. This chapter discusses client connectivity to the Firebox SSL VPN Gateway.

Before reading the examples in this chapter, you should become familiar with the settings on three tabs of the Administration Tool. The settings on these tabs control user access to internal network resources:

- Global Cluster Policies
- Authentication
- Access Policy Manager

The three user access configuration examples discussed in this chapter are:

- "Scenario 1: Configuring LDAP Authentication and Authorization" on page 160**.** This step-by-step example illustrates how an administrator might provide access to internal network resources in an LDAP environment.
- "Scenario 2: Creating Guest Accounts Using the Local Users List" on page 169**.** This example extends the scenario for configuring LDAP authentication and authorization to illustrate the concept of local users.
- "Scenario 3: Configuring Local Authorization for Local Users" on page 172**.** This example illustrates the concept of local authorization by slightly altering the configuration discussed in the scenario for creating guest accounts using the Local Users list.

Scenario 1: Configuring LDAP Authentication and Authorization

This example shows how an administrator might use the settings in the Administration Tool to configure user access in the following example scenario:

- The organization uses a single LDAP directory as the user repository
- Remote users working for the Sales department must have access to an email server, a Web conference server, a Sales Web application, and several file servers residing on the internal network
- Remote users working for the Engineering department must have access to an email server, a Web conference server, and several file servers residing on the internal network
- Three email servers are operating in the internal network, but the administrator wants remote users to access only one of these email servers

To configure access to the internal network resources in this scenario, the administrator completes two basic tasks:

- Preparing for the LDAP authentication and authorization configuration
- Configuring the Firebox SSL VPN Gateway to support access to the internal network resources

Each of these tasks is discussed below.

Preparing for the LDAP Authentication and Authorization Configuration

Preparing for the LDAP authentication and authorization configuration is the first of two tasks the administrator performs in the scenario for configuring LDAP authentication and authorization.

In this task, the administrator assembles the information needed to configure the Firebox SSL VPN Gateway to support LDAP authentication and authorization.

This task includes these procedures:

- Determining the internal networks that include the needed resources

- Determining the Sales and Engineering users who need remote access
- Collecting the LDAP directory information

Determining the internal networks that include the needed resources

Determining the internal networks that include the needed resources is the first of three procedures the administrator performs to prepare for the LDAP authentication and authorization configuration.

In this procedure, the administrator determines the network locations of the resources that the remote users must access. As noted earlier:

- Remote users working for the Sales department must have access to an email server, a Web conference server, a Sales Web application, and several file servers residing on the internal network
- Remote users working for the Engineering department must have access to an email server, a Web conference server, and several file servers residing on the internal network
- Three email servers are operating in the internal network, but the administrator wants remote users to access only one of these email servers

To complete this procedure in this example, we assume the administrator collects the following information:

- The Web conference server, email servers, and file servers that the remote Sales and Engineering users must access all reside in the network 10.10.0.0/ 24
- The server containing the Sales Web application resides in the network 10.60.10.0/24
- The single email server that remote users must access has the IP address 10.10.25.50

Determining the Sales and Engineering Users Who Need Remote Access

Determining the Sales and Engineering users who need remote access is the second of three procedures the administrator performs to prepare for LDAP authentication and authorization configuration.

Before an administrator can configure the Firebox SSL VPN Gateway to support authorization with an LDAP directory, the administrator must understand how the Firebox SSL VPN Gateway uses groups to perform the authorization process.

Specifically, the administrator must understand the relationship between a user's group membership in the LDAP directory and a user's group membership on the Firebox SSL VPN Gateway.

Note

The Firebox SSL VPN Gateway also relies on user groups in a similar way to support authorization types such as RADIUS.

When a user in an LDAP directory connects to the Firebox SSL VPN Gateway, the following basic authentication and authorization sequence occurs:

- After a user enters authentication credentials from the LDAP directory, the Firebox SSL VPN Gateway looks the user up in the LDAP directory, verifies the user's credentials, and logs the user on.
- After a user successfully authenticates, the Firebox SSL VPN Gateway examines an attribute in the user's LDAP directory Person entry to determine the LDAP directory groups to which the user belongs.

For example, if the Firebox SSL VPN Gateway operates with the Microsoft Active Directory, the Firebox SSL VPN Gateway checks the "memberOf" attribute in the Person entry to determine the groups to which a user belongs.

In this example, we assume that the group membership attribute indicates that a user is a member of an LDAP directory group named "Remote Sales."

The Firebox SSL VPN Gateway then looks for a user group configured on the Access Policy Manager tab of the Administration Tool that has a name that matches the name of an LDAP directory group to which the user belongs.

In this example, the Firebox SSL VPN Gateway looks for a user group named "Remote Sales" configured on the Firebox SSL VPN Gateway.

If the Firebox SSL VPN Gateway finds a user group configured on the Firebox SSL VPN Gateway that has the same name as an LDAP directory group to which the user belongs, the Firebox SSL VPN Gateway grants the user with the access privileges (authorization) assigned to the user group on the Firebox SSL VPN Gateway.

In this example, the Firebox SSL VPN Gateway provides the user with the access levels associated with the "Remote Sales" user group on the Access Policy Manager tab of the Administration Tool.

Therefore, before the administrator can authorize the Sales and Engineering users to access internal network resources through the Firebox SSL VPN Gateway, the administrator must know the LDAP directory groups to which these users belong.

At this point in this user access scenario, the administrator must accomplish one of two things regarding the group membership of the users:

- Identify groups on the LDAP directory that contain all of the members who need remote access to the internal networks
- If there are no existing groups that contain all of the appropriate members, the administrator can create new groups in the LDAP directory and add the appropriate members to these groups

In this example, we assume that the administrator creates groups named "Remote Sales" and "Remote Engineers" in the LDAP directory and populates these groups with the Sales and Engineering users that need remote access to the internal network resources.

Collecting the LDAP Directory Information

Collecting the LDAP directory information is the last of three procedures the administrator performs to prepare for the LDAP authentication and authorization configuration.

In this example scenario, the organization uses a single LDAP directory as its user repository.

Before the administrator can configure the Firebox SSL VPN Gateway to support authentication and authorization with an LDAP directory, the administrator must collect information about the LDAP directory. This information is used in a later procedure to configure the Firebox SSL VPN Gateway to connect to the LDAP directory to perform user and group name lookups.

Note

To determine the information needed to configure a particular authentication or authorization type click the Authentication tab in the Administration Tool and create a test authentication realm that includes the authentication and authorization types that you must support. Collect the information needed to complete the fields for the selected authentication and authorization types.

In this procedure, the administrator collects the following information about the LDAP directory.

- LDAP Server IP address. The IP address of the computer running the LDAP server.

- LDAP Server port. The port on which the LDAP server listens for connections. The default port for LDAP connections is port 389.
- LDAP Administrator Bind DN and LDAP Administrator Password. If the LDAP directory requires applications to authenticate when accessing it, the administrator must know the name of the user account that the Firebox SSL VPN Gateway should use for this authentication and the password associated with this account.
- LDAP Base DN. The base object of the directory (or level of the directory) where user names are stored. All remote users must have a Person entry at this level of the directory. Some example values are:
  ou=Users,dc=ace,dc=com
  cn=Users,dc=ace,dc=com
- LDAP Server login name attribute. The attribute of an LDAP directory Person entry that contains a user's name. The following table contains examples of the user name attribute fields for different LDAP directories:

LDAP Server	User Attributes	Case Sensitive
Microsoft Active Directory Server	sAM AccountName	No
Novell eDirectory	cn	Yes
IBM Directory Server	uid	
Lotus Domino	CN	
Sun ONE directory (formerly iPlanet)	uid or cn	Yes

- LDAP Group attribute - The attribute of a user's Person entry that lists the groups to which a user belongs; for example, "memberOf." The LDAP Group attribute is used only for LDAP authorization.
  At this point, the administrator has completed all of the procedures needed to prepare for the LDAP authentication and authorization configuration task. When this task is complete, the administrator has the following information:
- The specific network locations of all network resources that the remote Sales and Engineering users must access
- The names of the user groups in the LDAP directory that contain the Sales and Engineering users who require remote access ("Remote Sales" and "Remote Engineers" in this example)
- The specific LDAP directory information needed to configure the Firebox SSL VPN Gateway to operate with the LDAP directory

With this information available, the administrator is now ready to configure the Firebox SSL VPN Gateway to provide access to the internal network resources for the Sales and Engineering users.

Configuring the Firebox SSL VPN Gateway to Support Access to the Internal Network Resources

Configuring the Firebox SSL VPN Gateway to support access to the internal network resources is the last of two tasks the administrator performs in the scenario for configuring LDAP authentication and authorization.

In this task, the administrator uses the information gathered in the previous task to configure the settings in the Administration Tool that enable the remote users to access the internal network resources.

This task includes these five procedures:

- Configuring accessible networks
- Creating an LDAP authentication realm
- Creating the appropriate groups on the Firebox SSL VPN Gateway
- Creating and assigning network resources to the user groups
- Creating an application policy for the email server

Each of these procedures is discussed in detail below.

Configuring Accessible Networks

Configuring accessible networks is the first of five procedures the administrator performs to configure access to the internal network resources in the configuring LDAP authentication and authorization scenario.

In this procedure, the administrator specifies the internal networks that contain the network resources that users must access using the Secure Access Client.

In the previous task, the administrator determined that the remote Sales and Engineering users must have access to the resources on these specific internal networks:

- The Web conference server, file servers, and email server residing in the network 10.10.0.0/24
- The server containing the Sales Web application residing in the network 10.60.10.0/24

The administrator specifies these networks as accessible networks. Specifying the accessible networks enables the Secure Access Client to support split tunneling.

When a user logs on to the Firebox SSL VPN Gateway, the Firebox SSL VPN Gateway sends this list of networks to the Secure Access Client on the user's computer. The Secure Access Client uses this list of networks as a filter to determine which outbound packets should be sent to the Firebox SSL VPN Gateway and which should be sent elsewhere. The Secure Access Client transmits only the packets bound for the Firebox SSL VPN Gateway through the secure tunnel to the Firebox SSL VPN Gateway.

Note

If you do not want to support split tunneling, you do not need to configure accessible networks.

To configure accessible networks

1 Open the Administration Tool.

2 Click the **Global Cluster Policies** tab.

3 If necessary, select **Enable split tunneling**.

4 In the **Accessible networks** box, enter all of the internal networks that the Firebox SSL VPN Gateway must access. Separate each network entered with a space or a carriage return. In this example access scenario, the administrator would make these entries:
10.10.0.0/24
10.60.10.0/24

5 Select the **Enable logon page authentication** check box. This setting requires users to authenticate when accessing the portal page of the Firebox SSL VPN Gateway with a Web browser.

6 To simplify this example, assume the administrator clears all other check boxes that appear on the **Global Cluster Policies** tab.

For more information about split tunneling, see "Enabling Split Tunneling" on page 57.

For more information about the **Deny Access without ACL** setting, see "Denying Access to Groups without an ACL" on page 58.

Creating an LDAP Authentication and Authorization Realm

Creating an LDAP authentication and authorization realm is the second of five procedures the administrator performs to configure access to the internal network resources in this scenario.

In this scenario, all of the Sales and Engineering users are listed in a corporate LDAP directory.

To authenticate users listed in an LDAP directory, the administrator must create an authentication realm that supports LDAP authentication.

To authorize users listed in LDAP directory groups to access the internal network resources, the administrator selects LDAP Authorization as the authorization type of the realm.

Because all of the users authenticate to the LDAP directory, the administrator sets up the Default authentication realm to support LDAP authentication and authorization.

To set up the Default realm to support LDAP authentication, the administrator first deletes the existing Default realm and then immediately creates a new Default realm that supports LDAP authentication. This new realm includes the address, port, and other LDAP directory information that the Firebox SSL VPN Gateway needs to connect to the LDAP directory server and resolve searches for names in the directory.

Note

The existing Default realm on the Firebox SSL VPN Gateway is configured for local authentication. By deleting the existing Default realm and creating a new Default realm for LDAP, the administrator simplifies the logon process for the end user. Users who authenticate using the Default realm do not need to enter the realm name as part of their logon credentials. For more information about realms, authentication, and authorization, see "Configuring Authentication and Authorization" on page 61.

To complete this procedure, the administrator must have available the LDAP directory information gathered in the procedure "Collecting the LDAP Directory Information" on page 162" in the previous task.

To delete the existing Default realm and create a new Default realm that supports LDAP authentication and authorization

1. In the Firebox SSL VPN Gateway Administration Tool, click the **Authentication** tab.
2. Open the window for the Default realm.
3. On the **Action** menu, select **Remove "Default" realm**. A warning message appears.
4. Click **Yes**.
5. In **Realm Name**, type **Default**.
6. Select **One Source** and click **Add**.
7. At **Select Authentication Type**, select **LDAP authentication** and then click **OK**.
   The new Default realm window opens.
8. In the **Authentication** tab of the new Default realm window, complete the fields that enable the Firebox SSL VPN Gateway to access the LDAP server. (Use the information gathered in the procedure "Collecting the LDAP Directory Information" on page 162 in the previous task to complete these fields).
9. Select the **Authorization** tab.
10. In **Authorization type**, select **LDAP authorization**.
11. In the **Authorization** tab, complete the fields that enable the Firebox SSL VPN Gateway to access the LDAP server.
12. Click **Submit**.
    For more information about creating realms, see "Creating Additional Realms" on page 66.

Creating the Appropriate Groups on the Firebox SSL VPN Gateway

Creating the appropriate groups on the Firebox SSL VPN Gateway is the third of five procedures the administrator performs to configure access to the internal network resources in the configuring LDAP authentication and authorization scenario.

In this step, the administrator creates user groups on the Firebox SSL VPN Gateway that have names that match the groups the administrator identified or created in the LDAP directory.

In an earlier task, the administrator created LDAP directory groups named “Remote Sales” and “Remote Engineers” in the LDAP directory.

In this step, the administrator must now create user groups named “Remote Sales” and “Remote Engineers” on the Firebox SSL VPN Gateway.

1 Click the **Access Policy Manager** tab.

2 In the left pane, right-click **User Groups** and then click **New Group**.
In **Group Name**, type a name that is an exact case-sensitive match to an LDAP directory group that was identified or created in the earlier procedure.
For example, type "Remote Sales" and then click **OK**.

3 At this point, a **Group Properties** window appears that includes several tabs. To simplify this example, accept all of the default settings for the Group Properties and click **OK**.

The group properties provide additional settings that affect user access. For more information, about group properties and creating local groups, see “Configuring Properties for a User Group” on page 90.

Creating and Assigning Network Resources to the User Groups

Creating and assigning network resources to the user groups is the fourth of five procedures the administrator performs to configure access to the internal network resources in the configuring LDAP authentication and authorization scenario.

In this step, the administrator specifies the network resources (network segments or individual computers) that users can access and then assigns those resources to the user groups on the Firebox SSL VPN Gateway.

To complete this step, the administrator does the following:

- Creates a network resource named "Sales Resource" and assigns this resource to the "Remote Sales" user group
- Creates a network resource named "Engineering Resource" and assigns this resource to the "Remote Engineers" user group

Creating and Assigning Network Resources to the Sales Users

This section briefly discusses how the administrator creates a network resource for the Sales users and assigns it to those users.

As noted earlier, the Sales users need access to these systems:

- An email server, Web conference server, and several file servers in the 10.10.0.0/24 network.
- A Sales Web application in the 10.60.10.0/24 network.

To create a network resource named "Sales Resource" for the Sales users

1 Click the **Access Policy Manager** tab.

2 In the right pane, right-click **Network Resources** and then click **New Network Resource**.

3 Type "Sales Resources" as the Network Resource Name, and click **OK**.

4 In **Network/Subnet**, type these two IP address/subnet pairs for the resources. Separate each of these IP address/subnet pairs with a space:
10.10.0.0/24 10.60.10.0/24

5 To simplify this example, the administrator accepts the default values for the other settings on the **Network Resource** window and clicks **OK**.

After creating the Network Resource named "Sales Resource," the administrator uses the procedure below to add this network resource to the ACL of the "Remote Sales" user group.

1 From the Firebox SSL VPN Gateway Administration Tool, click the **Access Policy Manager** tab.

2 In the left-pane, expand **User Groups**, and then expand the "Remote Sales" user group.

3 In the right pane, expand **Network Resources**.

4 Click the "Sales Resource" network resource and drag it to **Network Policies** beneath the "Remote Sales" user group in the left-hand pane.

With this action, the administrator grants the users associated with the "Remote Sales" user group access to the systems defined in the network resource named "Sales Resources."

Note

In the procedure above, the administrator assigned the "Sales Resource" network resource to the access control list (ACL) of the "Remote Sales" user group. The administrator creates ACLs on the Firebox SSL VPN Gateway by adding resources to the network policies, application policies, kiosk policies, and end point policies associated with the user group. The ACL is comprised of all policies that are assigned to a user group on the Firebox SSL VPN Gateway.

Creating and Assigning Network Resources to the Engineering users

This section briefly discusses how the administrator creates a network resource and assigns it to the Engineering users. This procedure is essentially the same as the procedure completed for the Sales users in the previous step, except the administrator does not provide the engineering users with access to the Sales Web application in the 10.60.10.0/24 network.

As noted earlier, the Engineering users need access to a Web conference server, an email server, and several file servers. All of these servers reside in the network 10.10.0.0/24.

To provide the Engineering users with access to the network:

1 From the right pane of the **Access Policy Manager** tab in the Firebox SSL VPN Gateway Administration Tool, create a new network resource named "Engineering Resources." Specify only the 10.10.0.0/24 network when creating this resource.

2 In the left pane, expand the "Remote Engineers" user group.

3 Drag the "Engineering Resources" network resource from the right pane of the **Access Policy Manager** tab to the **Network Policies** of the "Remote Engineers" group in the left pane.

The "Engineering Resources" Network Resource is now part of the ACL for the "Remote Engineers" group.

Note

In more complex environments, it may be necessary to restrict access to a particular segment of a larger network. For example, an administrator may need to deny access to the 10.0.20.x network while allowing access to everything else in the 10.0.x.x network. The administrator creates a network resource for the 10.0.20.x network and a network resource for the 10.0.x.x network and assigns both network resources to the user group. The administrator then right-clicks each of the resources to deny access to

the 10.0.20.x resource and allow access to the 10.0.x.x resource.
In these cases, configure the policy denying access to 10.0.20.x first and then configure the policy allowing access to the 10.0.x.x network second. Always configure the most restrictive policy first and the least restrictive policy last.

Creating an Application Policy for an Email Server

Creating an application policy for an email server is the last of five procedures the administrator performs to configure access to the internal network resources in the configuring LDAP authentication and authorization scenario.

In this example, the network 10.10.0.0/24 contains three email servers, but the administrator wants the remote Sales and Engineering users to have access to only one of these email servers. The email server that remote users must access has the IP address 10.10.25.50/32.

To enable users to access only a single email server, the administrator creates an application policy on the Firebox SSL VPN Gateway that enables the users to access only the email application on the 10.10.25.50/32 email server.

Note

An administrator uses application policies to require a client application to access a specific internal server or to require a client device to meet specific requirements before it is allowed to access an internal server.

To create an application policy to restrict email client access to one server, the administrator must perform three actions:

- Create a network resource that includes only the email server
- Create an application policy that specifies the email application on the email server and assign the network resource containing the email server to this application policy
- Assign the application policy to the user groups in the Firebox SSL VPN Gateway

In this example, the administrator creates a network resource named "Email Server" that includes only IP address 10.10.25.50/32 (the email server). The administrator then creates an application policy named "Email Application Policy" that specifies the email application that remote users can access. The administrator assigns the "Email Server" network resource to this application policy.

Next, the administrator adds the "Email Application Policy" to the Remote Sales and Remote Engineers groups. Adding the policy to those groups ensures that those groups always access the email application on the specific email server specified by the administrator in the application policy.

To implement the application policy for the email server

1. From the right pane of the **Access Policy Manager** tab in the Firebox SSL VPN Gateway Administration Tool, create a new network resource named "Email server." For this Network Resource, specify only the IP address of the email server that users are allowed to access (for example, 10.10.25.50/ 32). This is the same basic procedure that was used to define the network resources for the Sales users and Engineering users in the previous procedures.
2. In the right pane, right-click **Application Policies** and then click **New Application Policies**.
3. In **Application Resource Name**, type "Email Application Policy" and click **OK**.
4. Browse to and select the email application located on the server that has the IP address 10.10.25.50/32.

The MD5 field is populated automatically with the binary sum of the application.

5 In the left pane, click the "Email server" network resource you just created and drag it to **Application Network Policies** listed under **Application Constraints** in the right pane. Click **OK**.

6 In the left pane, expand both the "Remote Sales" user group and the "Remote Engineers" user group.

7 In the right pane, under **Application Policies**, click the "Email Application Policy" and drag it to **Application Policies** under the Remote Sales user group in the left pane, so that the Application Policy is part of the Remote Sales ACL.

8 In the right pane, under **Application Policies**, click the "Email Application Policy" and drag it to **Application Policies** under the Remote Engineers user group in the left pane, so that the Application Policy is part of the Remote Engineers ACL.

Note

In the procedure above, the administrator could also add an application end point policy to the application policy to require every client device to meet specific requirements when accessing the email server. For more information, see "Application policies" on page 101.

This procedure concludes the scenario for configuring LDAP authentication and authorization.

When this procedure is complete, the administrator has configured all of the following:

- Users can authenticate to the LDAP directory specified in the Default authentication realm using their LDAP directory credentials.
- Users are authorized to access the internal network resources based on their group memberships in the LDAP directory and on the Firebox SSL VPN Gateway.

Only users who are members of the "Remote Sales" group and the "Remote Engineers" group are authorized to access resources on the internal network. (Each of these groups must exist both in the LDAP directory and on the Firebox SSL VPN Gateway.)

- Users in the "Remote Sales" group are authorized to access the Web conference server and file servers in the 10.10.0.0/24 network and the Sales Web application in the 10.60.10.0/24 network.

The Sales users can access the email application on the server with the 10.10.25.50 IP address, but cannot access the email application on other email servers in the allowed networks.

The Sales users can also access other network resources located in the two allowed networks.

- Users in the "Remote Engineering" group can access the Web conference server and the file servers in the 10.10.0.0/24 network (and other network resources located in this network).

The Engineering users can also access the email application on the server with the 10.10.25.50 IP address, but cannot access the email application on other email servers in the allowed networks.

To understand the purpose of local users on the Firebox SSL VPN Gateway and to understand how to enable authentication and authorization for the local users, continue to "Scenario 2: Creating Guest Accounts Using the Local Users List" on page 169.

Scenario 2: Creating Guest Accounts Using the Local Users List

This example illustrates how local users work on the Firebox SSL VPN Gateway and shows one way in which an administrator can support authentication and authorization for the local users.

In the previous example, users were authenticated and authorized based on their LDAP directory credentials and group memberships.

An administrator can also create a list of local users on the Firebox SSL VPN Gateway and configure the Firebox SSL VPN Gateway to provide authentication and authorization services for these users. This list of local users is maintained in a database on the Firebox SSL VPN Gateway and not in an external directory.

Local users are especially useful if the administrator wants to do any of the following:

- Grant access to users who are not listed in any corporate directory
- Grant access to users who are listed in a corporate directory to which the Firebox SSL VPN Gateway does not connect
- Provide a small number of users with a special level of access to the internal network resources without creating a new group in the corporate directory for these users

This example assumes the following:

- Silvio Branco and Lisa Marth are consultants that do not work for the corporation and are not listed in the corporate directory
- Silvio Branco and Lisa Marth must have remote access to the Web conference server on the internal network to participate in conferences with the Sales and Engineering users who are employed by the corporation
- The administrator has already completed the previous LDAP authentication with LDAP authorization example scenario earlier in this chapter to provide Sales and Engineering users with access to the Web conference server
- The Web conference server IP address is 10.10.50.60

Note

In this example, Silvio Branco and Lisa Marth are referred to as guest users because they are not employed by the corporation and are not listed in the corporate directory.

To provide Silvio Branco and Lisa Marth with access to the Web conference server, the administrator performs these three procedures:

- Creates a guest user authentication realm
- Creates local users
- Creates and assigns a network resource to the Default user group on the Firebox SSL VPN Gateway

Creating a Guest User Authentication Realm

Creating a guest user authentication realm is the first of three procedures the administrator performs in the scenario for creating guest accounts using the Local Users list.

In the previous scenario for configuring LDAP authentication and authorization, the administrator created a Default authentication realm to support authentication and authorization of the users listed in a corporate LDAP directory.

Because Silvio Branco and Lisa Marth are not listed in the corporate LDAP directory, the administrator creates a separate authentication realm for them that supports the following:

- Local Authentication. This option in an authentication realm ensures that users are authenticated against a Local Users list on the Firebox SSL VPN Gateway, and not an external directory
- No Authorization. This option in an authentication realm ensures that users of this realm are provided with the access levels associated with the Default user group on the Firebox SSL VPN Gateway.

To create a guest authentication realm for the guest users

1 In the Firebox SSL VPN Gateway Administration Tool, click the **Authentication** tab.

2 In **Realm Name**, type Guest.

3 Select **One Source** and click **Add**.

4 At **Select Authentication Type**, select **Local authentication only** and then click **OK**.

5 From the **Authorization** tab, select **No authorization**.

6 Click **Submit**.

Creating Local Users

Creating local users is the second of three procedures the administrator performs in the scenario for creating guest accounts using the Local Users list.

In this procedure, the administrator creates local user accounts for Silvio Branco and Lisa Marth on the Firebox SSL VPN Gateway and provides each user with a password.

To add the local users

1 Click the **Access Policy Manager** tab.

2 Right-click **Local Users** and select **New User**.

3 In **User Name**, type Lisa Marth.

4 In the **Password** and **Verify Password** fields, enter a password for Lisa Marth and click OK.

5 Repeat Steps 2 through 4 for to create a local user account for Silvio Branco.

Creating and Assigning a Network Resource to the Default User Group

Creating and assigning a network resource to the Default user group is the last of three procedures in the scenario for creating guest accounts using the Local Users list.

In this step, the administrator creates a network resource that specifies only the Web conference server and then assigns this resource to the Default user group.

1 From the right pane of the **Access Policy Manager** tab in the Administration Tool, create a new network resource named "Guest Resource." Specify only the IP address of the Web conference server when creating this network resource (for example 10.10.50.60/32).

2 In the left pane, expand the "Default" user group.

3 Drag the "Guest Resource" network resource from the right pane of the **Access Policy Manager** tab to the **Network Policies** of the "Default" group in the left pane.

Note

If a user logs on and cannot get group information, the user will always use the Default group settings.

When this procedure is complete, the administrator has accomplished the following:

- Silvio Branco and Lisa Marth can enter the user credential "Guest\Silvio Branco" or "Guest\Lisa Marth" to authenticate to the Guest realm on the Firebox SSL VPN Gateway. Silvio and Lisa must include the realm name as part of their user name credential when authenticating because they authenticate to a realm that is not the Default authentication realm.
- Silvio and Lisa also use the passwords that the administrator specified for them to authenticate to the Firebox SSL VPN Gateway. The administrator entered these passwords when creating Silvio and Lisa as local users on the Firebox SSL VPN Gateway.

Silvio and Lisa are authorized to access any resource defined in the ACL of the Default user group because No Authorization is specified as the authorization type of the Guest realm.

In this example, Silvio and Lisa can access only the Web conference server on the internal network because that is the only network resource defined for the Default user group.

Scenario 3: Configuring Local Authorization for Local Users

By slightly altering the configuration discussed previously in the "Scenario for Creating Guest Accounts Using the Local Users List", the administrator can provide local users (Lisa Marth and Silvio Branco) with the same level of access to the internal network resources as either the Sales or the Engineering users.

This scenario illustrates the concept of local authorization for local users.

Assume the administrator wants to provide Lisa and Silvio with the same level of access as the Engineering users. To accomplish this, the administrator could perform two procedures:

- Change the authorization type of the Guest realm to Local Authorization
- Assign the local users Lisa Marth and Silvio Branco to the Remote Engineers group on the Firebox SSL VPN Gateway

To assign local users Lisa Marth and Silvio Branco to the Remote Engineers group on the Firebox SSL VPN Gateway, the administrator performs this procedure:

1 Click the **Access Policy Manager** tab.

2 Expand **User Groups** and then expand **Local Users**.

3 Under **Local Users**, click the name Lisa Marth and drag her name to **Local Group Users** underneath the Remote Engineers user group.

4 Under **Local Users**, click the name Silvio Branco and drag his name to **Local Group Users** underneath the Remote Engineers user group.

When this procedure is complete, both of the following are true:

- Silvio Branco and Lisa Marth can enter the user credential "Guest\Silvio Branco" or "Guest\Lisa Marth" to authenticate to the Guest realm on the Firebox SSL VPN Gateway.
- Silvio and Lisa are authorized to access any resource defined in the ACL of the Remote Engineers user group because Local Authorization is specified as the authorization type of the Guest realm.

When Local Authorization is specified, local users receive the authorization associated with the user group on the Firebox SSL VPN Gateway to which they are assigned. They do not receive the authorization associated with the Default user group on the Firebox SSL VPN Gateway, as is the case when No Authorization is selected for the Guest authentication realm.

APPENDIX E

Legal and Copyright Information

GNU GENERAL PUBLIC LICENSE FOR LINUX KERNEL AS
PROVIDED WITH FIREBOX SSL Firebox SSL VPN Gateway
Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any

change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program

or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for

such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright

notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute

the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program

itself is interactive but does not normally print such an announcement, your work based on the Program is not required to

print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the

terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your

cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to

be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This
alternative is allowed only for noncommercial distribution and only if you received the program in object code or
executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) 19yy <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License
as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the
implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General
Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free
Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X

Z